

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

**НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
«ХАРКІВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ»**

*Євсєєв С.П., Дженюк Н.В., Толкачов М.Ю.,
Король О.Г., Воропай Н.І.*

КОМП'ЮТЕРНІ МЕРЕЖІ

Книга 1. Технології комп'ютерних мереж

Навчальний посібник

Харків – НТУ «ХПІ»
Львів – Видавництво ПП «Новий Світ – 2000»
2023

УДК 004.7(075)

Т 38

Вченою Радою Національного технічного університету
«Харківський політехнічний інститут» як навчальний посібник
для студентів галузей 12 – «Інформаційні технології» та 17 – «Електроніка,
автоматизація та електронні комунікації»
(протокол № 6 від 07.07.2023 року).

Рецензенти:

Казакова Н.Ф., д.т.н., проф., завідувач кафедри інформаційних технологій
Одеський державний екологічний університет

Остапов С.Е., д.ф-м.н., проф., завідувач кафедри програмного забезпечення
комп'ютерних систем Чернівецького національного університету
імені Ю.Федьковича

**Євсєєв С.П., Дженюк Н.В., Толкачов М.Ю.,
Король О.Г., Воропай Н.І.**

Т38 Комп'ютерні мережі. [Книга 1. Технології комп'ютерних мереж]:
[Навчальний посібник]. / Євсєєв С.П., Дженюк Н.В., Толкачов М.Ю та
ін. – Харків, – Львів: Видавництво ПП «Новий Світ – 2000», 2023. –
471 с. (Укр. мов.)

ISBN 978 – 966 – 418 – 399 – 1

Посібник містить теоретичні основи базових технологій і стандарти комп'ютерних мереж. Розглянуто базовий функціонал протоколів різних рівнів еталонної моделі OSI. Також розглянуті поняття комутації пакетів в мережі та IP-адресації. Наведено принципи та протоколи маршрутизації локальних та глобальних мереж. Описано стандартні стеки комутаційних протоколів. Розглянуто WAN-технології. Наведено стандарти та протоколи бездротових комп'ютерних мереж. Окремо розглянуто основи побудови безпеки в телекомунікаційних та комп'ютерних мережах.

Книга розрахована на студентів вищих навчальних закладів III-IV рівня акредитації, які навчаються в галузях 12 – «Інформаційні технології» та 17 – «Електроніка, автоматизація та електронні комунікації».

УДК 004.7(075)

ISBN 978 – 966 – 418 – 399 – 1

© Національний технічний університет
«Харківський політехнічний інститут», 2023
© Євсєєв С.П., Дженюк Н.В., Толкачов М.Ю.,
Король О.Г., Воропай Н.І., 2023
© Видавництво ПП «Новий Світ – 2000»,
ФОП Піча С.В., 2023

ВСТУП

Даний посібник призначений для поєднання сучасних технологій побудови інформаційно-комунікаційних мереж і принципів роботи їх складових елементів, а також технологій обробки інформації та забезпечення послуг безпеки.

Головним завданням системних інтеграторів та адміністраторів є оптимальне та ефективне управління інформаційно-комунікаційною мережею для ефективного вирішення завдань щодо обробки інформаційних потоків сучасних мереж підприємств та організацій [26; 43]. Постійне зростання об'ємів і потоків корпоративної інформації призводить до зміни технології її обробки. Зміна схем ведення документообігу, бізнесу або виробництва змінюють і вимоги до інформаційно-комунікаційних мереж, відомо, що строки морального старіння продуктів та рішень в галузі інформаційних технологій не перевищує 5 років [9; 43]. Інтенсивне звертання до послуг інформаційних ресурсів зовнішніх організацій підвищує навантаження на граничні маршрутизатори та мережеві екрани інформаційно-комунікаційних мереж, і як наслідок на підсистеми забезпечення безпеки інформації.

Постійні зміни та нові впровадження в сучасні комунікації вимагає від інженерно-технічного складу вдосконалення своїх знань та вмінь на основі існуючих.

Враховуючи сучасну динаміку розвитку телекомунікаційних технологій [38; 43] та вимоги до фахівців в галузі телекомунікації, в посібнику послідовно наведені базові технології локальних мереж, основні стандарти комп'ютерних мереж, стандартні стеки комутаційних протоколів, глобальні комп'ютерні мережі. У навчальному посібнику “Технології комп'ютерних мереж” розглянуто питання щодо побудови сучасних систем забезпечення інформаційної безпеки та захисту інформації в складних комп'ютерних та обчислювальних мережах. Велику увагу приділено викладанню національних та міжнародних стандартів криптографічного перетворення інформації і найбільш поширених криптографічних механізмів захисту та забезпечення безпеки інформаційних технологій.

РОЗДІЛ 1. БАЗОВІ ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ

1.1. Історія розвитку комп'ютерних мереж

Комп'ютерні мережі, звані також мережами передачі даних, є логічним результатом еволюції двох важливих науково-технічних галузей сучасної цивілізації. Комп'ютерні мережі є логічним результатом еволюції двох найважливіших науково-технічних галузей сучасної цивілізації – обчислювальної техніки та телекомунікаційних технологій.

З одного боку, комп'ютерні мережі являють собою групу комп'ютерів, які узгоджено вирішують набір взаємопов'язаних завдань, обмінюючись даними в автоматичному режимі. З іншого боку, комп'ютерні мережі можуть розглядатися як засіб передавання інформації на великі відстані, для чого в них застосовуються методи кодування і мультиплексування даних, що набули розвитку в різних телекомунікаційних системах, наприклад телефонних мережах.

Перші потужні комп'ютери 50-х років, так звані мейнфрейми, були дуже дорогими і призначалися тільки для пакетного оброблення даних. Пакетне оброблення даних – найефективніший режим використання процесора дорогої обчислювальної машини. З появою дешевших процесорів почали розвиватися інтерактивні термінальні системи розподілу часу на базі мейнфреймів. Термінальні мережі з'єднували мейнфрейми з терміналами. Термінал – це пристрій для взаємодії з обчислювальною машиною, яка складається із засобів введення, наприклад клавіатури, і засобів виведення інформації, наприклад дисплея. Самі термінали практично ніякого оброблення даних не здійснюють, а використовують можливості потужної і дорогої центральної електронно-обчислювальної машини (ЕОМ). Ця організація роботи називається "Режим розподілу часу", оскільки центральна ЕОМ послідовно в часі вирішує завдання безлічі користувачів. При цьому спільно використовуються дорогі обчислювальні ресурси. Віддалені термінали з'єднувалися з комп'ютерами в телефонних мережах за допомогою модемів. Такі мережі дозволяли численним користувачам одержувати віддалений доступ до розподілених ресурсів потужних ЕОМ. Потім потужні ЕОМ об'єднували між собою – так з'явилися глобальні обчислювальні мережі. Отже, спочатку мережі застосовувалися для передачі цифрових даних між терміналом і великою обчислювальною машиною. Перші локальні обчислювальні мережі (ЛОМ) з'явилися на початку 70-х років, коли були

випущені міні-комп'ютери. Міні-комп'ютери були набагато дешевші за мейнфрейми, що дозволило використовувати їх у структурних підрозділах підприємств. Потім з'явилася необхідність обміну даними між машинами різних підрозділів. Для цього багато підприємств стали з'єднувати свої мінікомп'ютери і розробляти програмне забезпечення, необхідне для їх взаємодії. У результаті з'явилися перші ЛОМ. Поява персональних комп'ютерів стала стимулом для подальшого розвитку ЛОМ. Вони були досить дешевими і були ідеальними елементами для побудови мереж. Розвитку ЛОМ сприяла поява стандартних технологій об'єднання комп'ютерів у мережах: Ethernet, Arcnet, Token Ring. Поява якісних ліній зв'язку забезпечила досить високу швидкість передачі даних – 10 Мбіт/с, тоді як глобальні мережі використовували тільки погано пристосовані для передачі даних телефонні канали зв'язку, мали низьку швидкість передачі – 1200 біт/с. Через таку відмінність у швидкостях багато технологій, застосовуваних у ЛОМ, були недоступні для використання в глобальних мережах. Сьогодні мережні технології інтенсивно розвиваються, і розрив між локальними і глобальними мережами скорочується, багато в чому завдяки появі високошвидкісних територіальних каналів зв'язку, що не поступаються за якістю кабельним системам ЛОМ. Нові технології зробили можливим передачу таких не властивих раніше обчислювальним мережам носіїв інформації, як голос, відеозображення і рисунки. Складність передачі мультимедійної інформації в мережі пов'язана з її чутливістю до затримок під час передачі пакетів даних (затримки зазвичай призводять до спотворення такої інформації в кінцевих вузлах зв'язку). Але ця проблема вирішується, і конвергенція телекомунікаційних мереж (радіо-, телефонних, телевізійних і обчислювальних мереж) відкриває нові можливості для передачі даних, голосу і зображення в глобальних мережах Інтернет [2].

1.2. Стандартизація в комп'ютерних мережах

Всі пристрої, що працюють в одній мережі передачі даних, повинні функціонувати відповідно до загальновизнаного алгоритму у форматі, що буде зрозумілим іншим пристроям. Однак, з розвитком мереж передачі даних, розходження в поглядах розроблювачів на фундаментальні основи мережі стали приводити до несумісності пристроїв. Найперші мережі взагалі були працездатні тільки за умови, що всі їхні компоненти поставлялися одним виробником. Це приводило до того, що замовники стали групуватися

навколо ведучих виробників, утворюючи як би клуби, вхід у які був закритий для прихильників інших фірм. При такому положенні речей заміна існуючого мережного обладнання продуктами інших виробників означала серйозні грошові витрати.

У зв'язку із цим, стандартизація в комп'ютерних мережах здобуває особливе значення. Суть мережі – це з'єднання різного обладнання, а виходить, проблема сумісності є однією з найбільш гострих. Без прийняття всіма виробниками загальноприйнятих правил побудови обладнання прогрес у справі будівництва мереж був би неможливий. Тому весь розвиток комп'ютерної галузі в остаточному підсумку відбито в стандартах – будь-яка нова технологія тільки тоді здобуває законний статус, коли її зміст закріплюється у відповідному стандарті.

У комп'ютерних мережах ідеологічною основою стандартизації є багаторівневий підхід до розробки засобів мережної взаємодії. Саме на основі цього підходу була розроблена стандартна семірівнева модель взаємодії відкритих систем, що стала свого роду універсальною мовою мережних фахівців.

Організація взаємодії між пристроями в мережі є складною задачею. Як відомо, для рішення складних задач використовується універсальний прийом – *декомпозиція*, тобто розбивка однієї складної задачі на трохи більш прості задачі-модулі [2].

При *декомпозиції* часто використовують багаторівневий підхід. Він полягає в наступному. Всю множину модулів розбивають на рівні. Рівні утворюють ієрархію, тобто є вищележачі та нижележачі рівні. Множина модулів, складових кожний рівень, сформовано таким чином, що для виконання своїх задач вони звертаються із запитом тільки до модулів безпосередньо примикає нижележачого рівня. З іншого боку, результати роботи всіх модулів, що належать деякому рівню, можуть бути передані тільки модулям сусіднього вищележачого рівня. Така ієрархічна задача припускає чітке визначення функції кожного рівня й інтерфейсів між рівнями. Інтерфейс визначає набір функцій, які нижележачий рівень надає вищележачому. У результаті ієрархічної побудови мережі досягається відносна незалежність рівнів, а виходить, і можливість їх легкої заміни.

На рис. 1.1 показана модель взаємодії двох вузлів. З кожної сторони засобу взаємодії представлені чотирма рівнями. Процедура взаємодії цих двох вузлів може бути описана у вигляді набору правил взаємодії кожної пари відповідних рівнів обох сторін, які беруть участь. Формалізовані

правила, що визначають послідовність і формат повідомлень, якими обмінюються мережні компоненти, що лежать на одному рівні, але в різних вузлах, називаються протоколом.

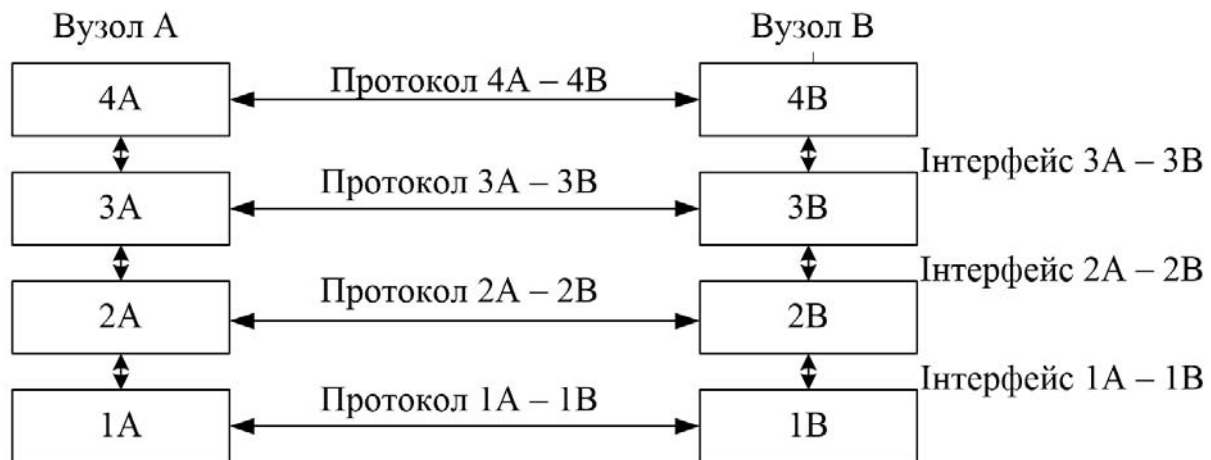


Рис. 1.1. Взаємодія двох вузлів

По суті, протокол і інтерфейс виражають те саме поняття, але традиційно в мережах за ними закріпили різні області дії: протоколи визначають правила взаємодії модулів одного рівня в різних вузлах, а інтерфейси – модулів сусідніх рівнів в одному вузлі.

Засоби кожного рівня повинні відпрацьовувати, по-перше, свій власний протокол, а по-друге, інтерфейси із сусідніми рівнями.

Ієрархічно організований набір протоколів, достатній для організації взаємодії вузлів у мережі, називається **стеком комунікаційних протоколів**. *Комунікаційні протоколи* можуть бути реалізовані як програмно, так і апаратно. *Протоколи нижніх рівнів* часто реалізуються комбінацією програмних і апаратних засобів, а протоколи верхніх рівнів – як правило, чисто програмними засобами.

Програмний модуль, що реалізує деякий протокол, часто для стислості також називають протоколом. При цьому співвідношення між протоколом – формально певною процедурою й протоколом – програмним модулем, що реалізує цю процедуру, аналогічно співвідношенню між алгоритмом рішення деякої задачі й програмою, що вирішує цю задачу [5].

Протоколи реалізуються не тільки комп'ютерами, але й іншими мережними пристроями – концентраторами, мостами, комутаторами, маршрутизаторами та інш. Дійсно, у загальному випадку зв'язок комп'ютерів у мережі здійснюється не прямо, а через різні комунікаційні пристрої.

Залежно від типу пристрою в ньому повинні бути убудовані засоби, що реалізують той або інший набір протоколів.

1.3. Основні організації, що займаються стандартизацією комп'ютерних мереж

У світі існує велика кількість розробників мереж, кожен з яких має уявлення про способи реалізації різних функцій. Без координації їх дій настала би повна плутанина, і користувачі не змогли б працювати. Єдиним способом боротьби з хаосом є досягнення згоди щодо певних питань на основі мережевих стандартів. Стандарти не тільки забезпечують можливість спілкування комп'ютерів, але також розширюють ринок для продукції, що дотримується стандарту, що призводить до масового випуску сумісної апаратури, дуже широкомасштабної інтеграції, здешевлення виробництва і, отже, ще більшого припливу споживачів на цей ринок. В даний час існує безліч спеціальних ділових організацій, які утворюються навколо деяких технологій і також відіграють істотну роль у розвитку та вдосконаленні мережевих стандартів.

У 1865 році представники багатьох європейських держав зібралися, щоб сформувати союз, який став попередником сьогоdnішнього *Міжнародного союзу телекомунікацій (ITU, International Telecommunications Union)*. Завданням цього союзу стала стандартизація міжнародних засобів зв'язку. На той час ще не було чого стандартизувати, крім телеграфу, але вже тоді було зрозуміло, що якщо половина країн використовуватиме абетку Морзе, а інша половина – якийсь інший код, то виникнуть проблеми. З появою міжнародного телефонного зв'язку ITU зайнявся розробкою стандартів у галузі телефонії. 1947 року міжнародний союз телекомунікацій увійшов до складу установ Організації Об'єднаних Націй.

У ITU входять приблизно 200 представників різних відомств, включаючи практично всі організації ООН. До складу ITU входить приблизно 700 представників відповідного промислового сектора та асоційовані члени, серед яких є і телефонні компанії (наприклад, AT&T, Vodafone, Sprint), і виробники телекомунікаційної апаратури (наприклад, Cisco, Nokia, Nortel), та виробники комп'ютерів (наприклад, Microsoft, Agilent, Toshiba), виробники мікросхем (наприклад Intel, Motorola, TI) та інші зацікавлені компанії (наприклад, Boeing, CBS, VerySign) [43].

У ІТУ є три основні сектори. *ITU-T, Телекомунікаційному секторі стандартизації*, що стосується систем передачі даних та телефонії. *ITU-R, Сектор радіозв'язку*, займається координуванням використання конкуруючими зацікавленими групами радіочастот у всьому світі.

Інший сектор – *ITU-D, Сектор розвитку*. Він сприяє розвитку інформаційно-комунікаційних технологій, щоб звузити «цифрову прірву» між країнами з ефективним доступом до інформаційних технологій та країнами з обмеженим доступом.

Завданням ІТУ-Т є розробка технічних рекомендацій у сфері телефонії, телеграфу та інтерфейсів передачі. Подібні рекомендації часто стають міжнародними стандартами, хоча технічно рекомендації ІТУ-Т є лише пропозиціями, які уряд будь-якої країни може прийняти або проігнорувати.

Міжнародні стандарти розробляються *Міжнародною організацією зі стандартизації (ISO)*, добровільною організацією, створеною в 1946 році. До неї входять національні організації зі стандартизації із 89 країн. Серед її членів ANSI (США), BSI (Великобританія), AFNOR (Франція), DIN (Німеччина) та ще 153 інші організації.

ISO випускає стандарти щодо широкого спектру питань, починаючи від болтів і гайок до фарбування телефонних стовпів (ISO 2451), рибальські мережі (ISO 1530), жіноча спідня білизна (ISO 4416)). Складно вигадати таку річ, для якої не існувало б стандарту ISO). З проблем телекомунікаційних стандартів Міжнародна організація зі стандартизації ISO та ІТУ-Т часто співпрацюють (ISO – член ІТУ-Т), щоб уникнути парадоксу двох офіційних та взаємно несумісних міжнародних стандартів.

На цей час випущено понад 17 000 стандартів, включаючи стандарти OSI. У ISO входять понад 200 технічних комітетів (Technical Committee, TC), нумерованих послідовно, з їх створення, кожен із яких займається своїм окремим питанням.

Національний інститут стандартів та технологій США (NIST, National Institute of Standards and Technology) є підрозділом Міністерства торгівлі США (U.S. Dept. of Commerce). Раніше він називався Національним бюро стандартів (National Bureau of Standards). Він випускає стандарти, обов'язкові для закупівель, які проводять уряд США, крім закупівель Міністерства оборони, яке визначає свої стандарти.

Ще однією організацією з стандартизації є *Інститут інженерів з електротехніки та електроніки (IEEE, Institute of Electrical and Electronics Engineers)* – найбільша професійна організація у світі. Окрім випуску ряду

журналів та організації різноманітних конференцій, IEEE також розробляє стандарти в галузі електротехніки та електроніки.

Всесвітня мережа Інтернет має свій механізм стандартизації, що значно відрізняється від ITU-T та ISO.

Коли було запущено мережу ARPANET, Міністерство оборони США створило не офіційний комітет спостереження за мережею. У 1983 році цей комітет був перейменований на *Раду з діяльності Інтернету (Internet Activities Board, IAB)*. Перед радою було поставлено кілька розширених завдань, а саме утримувати дослідників, включених у проекти ARPANET та Інтернет, у більш-менш одному напрямку. Значення скорочення IAB було змінено на *Раду з архітектури Інтернету (Internet Architecture Board)*.

Стандарти оформлялися як набору технічних звітів, званих *RFC (Requests for Comments)*. RFC доступні в Інтернеті всім бажаючим (www.ietf.org/rfc). Вони пронумеровані у хронологічному порядку їх створення.

До 1989 року Інтернет виріс настільки, що подібний неформальний підхід до його стандартів перестав працювати. До того моменту багато виробників пропонували продукцію на основі протоколу TCP/IP і не хотіли їх змінювати просто тому, що десятку дослідників спала на думку одна хороша ідея. Влітку 1989 року IAB було знову реорганізовано. Дослідники були переведені до *групи досліджень Інтернету (Internet Research Task Force, IRTF)*, підконтрольної IAB, і до *групи проектування Інтернету (Internet Engineering Task Force, IETF)*. У раді IAB з'явилися люди, які мають ширший спектр організацій, ніж дослідницьке співтовариство. Потім було створено *Товариство Інтернету (Internet Society)*, до якого увійшли люди, зацікавлені в Інтернеті. Ідея цього поділу полягала в тому, щоб зосередити IRTF на довгострокових дослідженнях, а IETF – на короткострокових інженерних питаннях. Проблемну групу IETF було поділено на робочі групи, кожна з яких вирішувала своє завдання [4].

1.4. Еталонна модель взаємодії відкритих систем

В процесі розвитку телекомунікаційної і інформаційної індустрії величезне значення відіграє стандартизація мережевого апаратного і програмного забезпечення. Без вхвалення всіма виробниками загальноприйнятих правил побудови елементів мережі вирішити проблему сумісності різного обладнання було б неможливо.

Багаторівневий підхід є ідеологічною основою стандартизації в мережах телекомунікацій. На основі цього підходу була розроблена так звана *еталонна модель взаємодії відкритих систем* (EMBC) або модель OSI (Open System Interconnection) [38]. Всі створювані мережі базуються на ідеях, що сформульовані в моделі OSI [26] і втілені у вигляді системи протоколів управління інформаційним обміном та реалізуються в мережевому програмно-апаратному забезпеченні.

Модель OSI створювалася рядом міжнародних організацій, що працюють у сфері стандартизації, серед яких Міжнародна організація зі стандартизації (ISO) і Міжнародний консультативний комітет з телефонії і телеграфії (нині Сектор телекомунікаційної стандартизації Міжнародного союзу електрозв'язку – ITU-T).

Модель OSI визначає різні рівні взаємодії систем в мережах з комутацією пакетів, дає їм стандартні назви і вказує функції, що ними виконуються. Ця модель, судячи з її назви, описує взаємодію відкритих систем. У широкому сенсі *відкритою системою* може бути названа будь-яка система, яка побудована відповідно до відкритих специфікацій.

Під терміном *специфікація* розуміють формалізований опис апаратних або програмних компонентів, способів їх функціонування, взаємодії, умов експлуатації та інших характеристик. Відкриті специфікації – це загальнодоступні, відповідні стандартам специфікації, прийняті в результаті всестороннього колективного обговорення. Використання систем з відкритими специфікаціями дозволяє:

- 1) істотно спростити освоєння цих систем;
- 2) забезпечити їх сполучення;
- 3) іншим компаніям розробляти і випускати для цих систем різні засоби їх модифікації і розширення;
- 4) створювати програмно-апаратні комплекси з продуктів різних виробників.

Відкритість систем, що функціонують відповідно до моделі OSI, полягає у відкритості засобів їх взаємодії. При цьому аспекти їх внутрішнього функціонування не обов'язково є відкритими. Таким чином, під відкритою системою, що функціонує в рамках моделі OSI, розуміється мережевий пристрій, здатний взаємодіяти з іншими мережевими пристроями з використанням стандартних правил, що регламентують процес інформаційного обміну.

Багаторівневий підхід при декомпозиції задачі взаємодії компонентів телекомунікаційної мережі. Будь-яка телекомунікаційна мережа є з'єднанням різного обладнання, різних мережевих пристроїв. Організація взаємодії між пристроями в мережі є складним завданням. Для вирішення складних завдань часто використовується універсальний прийом – декомпозиція.

Декомпозицією називається розбиття одного складного завдання на декілька простіших завдань-модулів. Процедура декомпозиції включає чітке визначення функцій кожного модуля, окремого завдання, що розв'язується, а також зв'язку між цими модулями. В результаті досягається логічне спрощення завдання, з'являється можливість його успішного рішення. Ідея модульної побудови складних технічних систем не раз з успіхом застосовувалася в електроніці, сфері програмного забезпечення, при розробці сучасних ЕОМ.

При реалізації декомпозиції часто застосовується *багаторівневий підхід*. Його суть полягає в тому, що всю множину модулів розбивають на рівні.

В рамках одного рівня групуються функціонально найбільш близькі компоненти. При цьому рівні утворюють ієрархію. Компоненти кожного рівня взаємодіють тільки з компонентами суміжних рівнів: до компонентів нижче розміщеного рівня звертаються із запитом, необхідними для вирішення своїх завдань, а компонентам вище розміщеного рівня передають результати своєї роботи.

Цей багаторівневий підхід успішно застосовується при декомпозиції завдання мережевої взаємодії. Компоненти мережі представляються при цьому у вигляді ієрархічно організованих модулів. Так, наприклад, модулі нижнього рівня можуть вирішувати задачу надійної передачі електричних сигналів між двома сусідніми вузлами. Модулі вищих рівнів реалізують транспортування повідомлень в межах всієї мережі. А на верхньому рівні працюють модулі, що надають доступ користувачам до різних мережевих служб, тобто безпосередньо контактують з людиною.

Розглянемо модель взаємодії засобів двох вузлів мережі А і Б (рис. 1.2). З кожного боку засобу взаємодії групуються в набір рівнів: від рівня № 1 до рівня № N.

Вся процедура взаємодії пункту А з пунктом Б може бути наведена у вигляді окремих правил взаємодії засобів, утворюючих відповідні рівні пунктів. Наприклад, компоненти 1-го рівня пункту А взаємодіють з

компонентами цього ж 1-го рівня пункту Б. Аналогічно відбувається взаємодія засобів 2-го і решти рівнів.

Формалізовані правила взаємодії мережевих компонентів одного і того ж рівня різних вузлів називаються *протоколом*.

Мережеві компоненти суміжних рівнів теж взаємодіють. Формалізовані правила взаємодії мережевих компонентів суміжних рівнів якого-небудь вузла отримали назву *інтерфейс*.

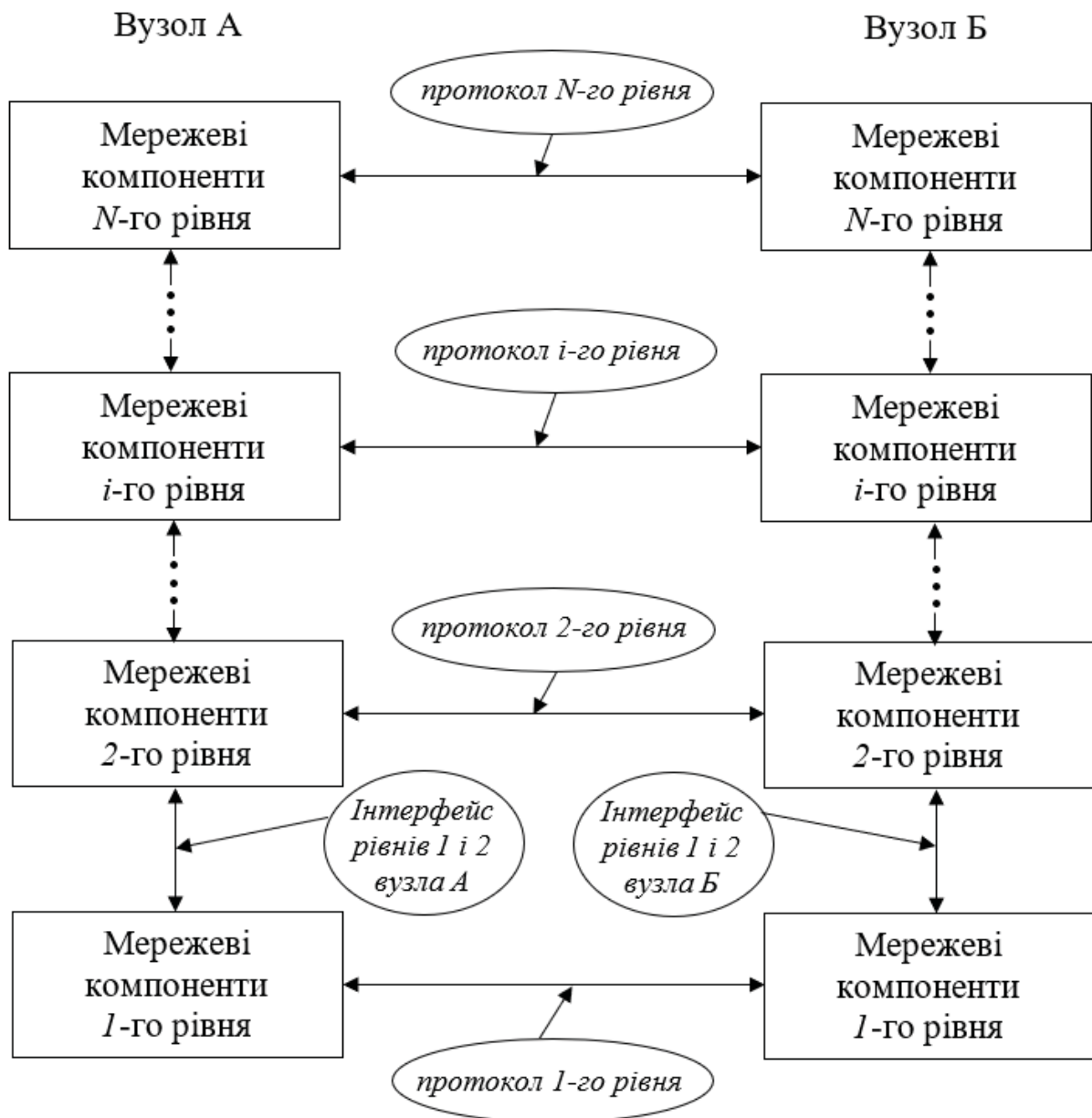


Рис. 1.2. Модель взаємодії засобів двох вузлів мережі

Таким чином, мережеві засоби кожного рівня повинні, по-перше, здійснювати взаємодію відповідно до протоколу свого рівня, а по-друге,

взаємодіяти із засобами суміжних рівнів відповідно до встановлених інтерфейсів.

Протоколи часто об'єднуються в стеки. *Стеком протоколів* називається ієрархічний набір протоколів, достатній для успішного здійснення взаємодії між вузлами мережі. Прикладами поширених стеків протоколів є TCP/IP, X.25 і ін.

Різні мережеві пристрої (комп'ютери, концентратори, комутатори, маршрутизатори і ін.) здійснюють взаємодію в мережі відповідно до тих або інших протоколів і інтерфейсів. Функції, що виконуються тими або іншими мережевими компонентами в процесі їх взаємодії, стандартизовані для кожного рівня.

У моделі OSI засоби взаємодії діляться на сім рівнів: *фізичний, канальний, мережевий, транспортний, сеансовий, представницький, прикладний* (рис. 1.3).

Розглянемо процес інформаційного обміну відповідно до моделі. Хай додаток звертається із запитом до прикладного рівня, наприклад, до файлової служби. На підставі цього запиту програмне забезпечення прикладного рівня формує повідомлення стандартного формату.

Звичайне повідомлення складається із заголовка і поля даних. Заголовок містить службову інформацію, яку необхідно передати через мережу прикладному рівню машини-адресата, щоб повідомити його, яку роботу треба виконати. У цьому випадку заголовок повинен містити інформацію про місце знаходження файлу та тип операції, яку необхідно над ним виконати. Поле даних несе в собі інформативний зміст повідомлення, наприклад, дані, які необхідно записати у віддалений файл. Але для того, щоб доставити цю інформацію за призначенням, належить вирішити ще багато завдань, виконуваних засобами нижче розташованих рівнів.

Після формування повідомлення прикладний рівень направляє його вниз в стек представницького рівня. Протокол представницького рівня на підставі інформації, одержаної із заголовка прикладного рівня, виконує необхідні дії і додає до повідомлення власну службову інформацію – заголовок представницького рівня, в якому містяться вказівки для протоколу представницького рівня машини-адресата.

В результаті одержане повідомлення передається вниз сеансовому рівню, який в свою чергу додає свій заголовок, і т.д. Нарешті, повідомлення досягає нижнього, фізичного рівня, який власне і передає його каналами

зв'язку машині-адресату. До цього моменту повідомлення “обростає” заголовками всіх рівнів.

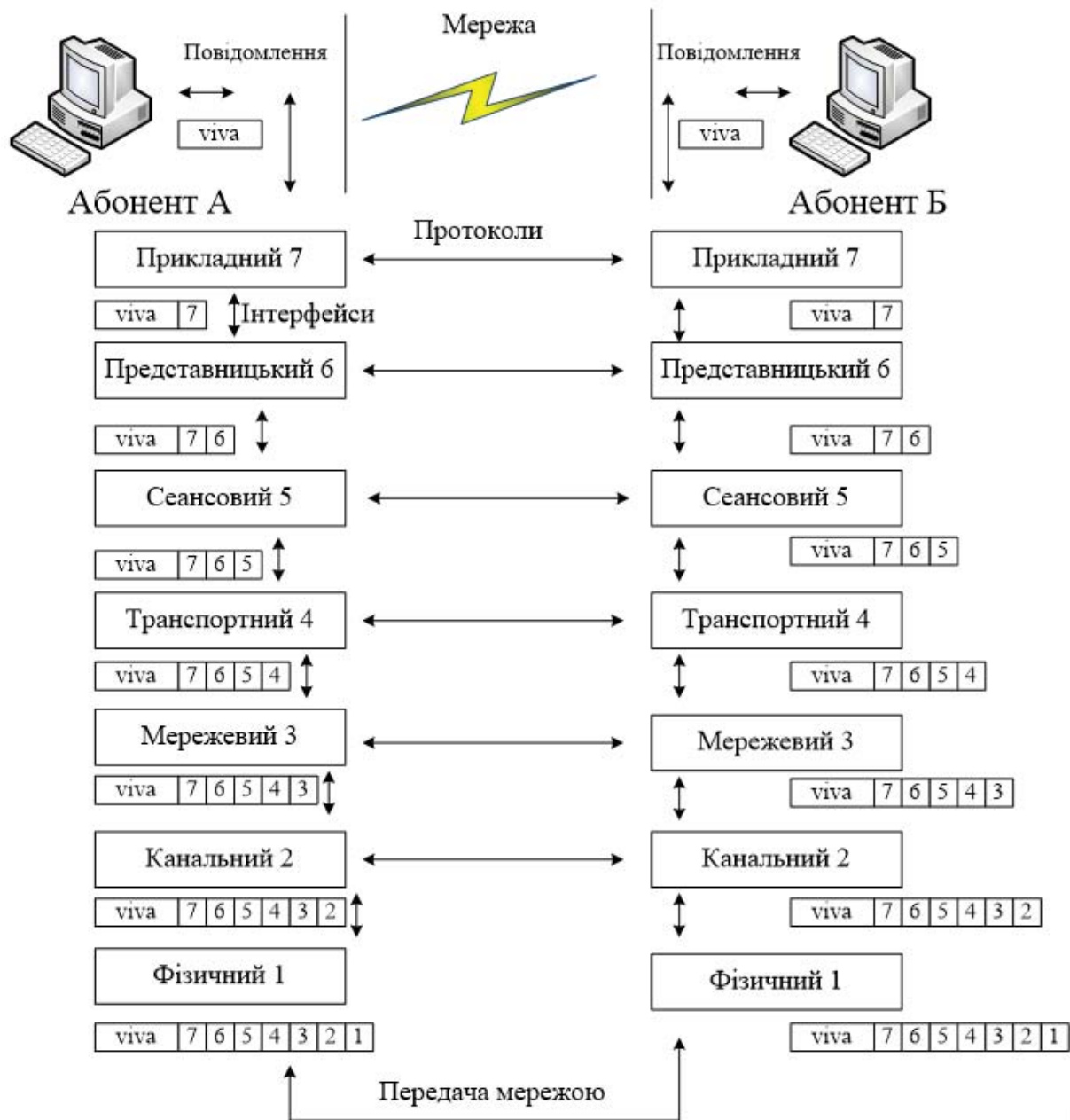


Рис. 1.3. Модель взаємодії відкритих систем

Рівні моделі OSI та їх характеристики. Розглянемо функції, що виконуються компонентами кожного з рівнів.

Фізичний рівень визначає особливості передачі сигналів фізичними каналами зв'язку. До цього рівня мають відношення характеристики фізичних середовищ передачі даних, такі як смуга пропускання, перешкодозахисна, хвильовий опір та інші. На цьому рівні визначаються

характеристики електричних сигналів, які передають дискретну інформацію, наприклад крутизну фронтів імпульсів, рівні напруги або струму сигналу, що передається, тип кодування, швидкість передачі сигналів. Окрім цього, тут стандартизуються типи з'єднувачів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку комп'ютера функції фізичного рівня виконуються мережевим адаптером або послідовним портом. Прикладом протоколу фізичного рівня може служити специфікація 10Base-T технології Ethernet, яка визначає, що для передачі буде використаний кабель неекранованої витвої пари категорії 3 з хвильовим опором 100 Ом; з'єднувач – RJ-45; максимальна довжина фізичного сегменту 100 м; манчестерський код для цифрового кодування даних, а також деякі інші характеристики середовища і електричних сигналів.

Одним із завдань *канального рівня* є перевірка доступності середовища передачі. Іншим завданням канального рівня є реалізація механізмів виявлення і корекції помилок. Для цього на канальному рівні біти групуються в набори, які мають назву *кадри*. Канальний рівень забезпечує коректність передачі кадрів. Для цього обчислюється контрольна сума, визначеним способом обробляються всі байти кадру і додається контрольна сума до кадру.

У локальних мережах протоколи канального рівня використовуються комп'ютерами, мостами, комутаторами і маршрутизаторами. У комп'ютерах функції канального рівня реалізуються спільними зусиллями мережевих адаптерів та їх драйверів. У глобальних мережах, які на відміну від локальних мереж рідко володіють регулярною топологією, канальний рівень забезпечує обмін повідомленнями тільки між двома сусідніми комп'ютерами, сполученими індивідуальною лінією зв'язку. Прикладами протоколів “точка-точка” (як часто називають такі протоколи) можуть служити широко поширені протоколи PPP і LAR-B.

Мережевий рівень служить для утворення єдиної транспортної системи, яка об'єднує декілька мереж, причому ці мережі можуть використовувати різні принципи передачі повідомлень між кінцевими вузлами і володіти довільною структурою зв'язку.

Мережі з'єднуються між собою спеціальними пристроями, що називаються маршрутизаторами. *Маршрутизатор* – це пристрій, який збирає інформацію про топологію міжмережєвих з'єднань і на її підставі пересилає пакети мережевого рівня в мережу призначення. Для того, щоб передати повідомлення мережевого рівня (пакети) від відправника, що знаходиться в одній мережі, одержувачу, який знаходиться в іншій мережі, потрібно

зробити деяку кількість транзитних передач між мережами. Таким чином, *маршрут* є послідовністю маршрутизаторів, через які проходить пакет. Проблема вибору найкращого шляху називається *маршрутизацією*, а її рішення є одним з головних завдань мережевого рівня.

Мережевий рівень вирішує також задачі узгодження різних технологій, спрощення адресації в великих мережах і створення надійних і гнучких бар'єрів на шляху небажаного трафіку між мережами. Прикладами протоколів мережевого рівня є протокол міжмережевої взаємодії IP стека TCP/IP і протокол міжмережевого обміну пакетами IPX стека Novell.

На шляху від відправника до одержувача пакети можуть бути спотворені або загублені. Робота *транспортного рівня* полягає в тому, щоб забезпечити додаткам або верхнім рівням стека – прикладному і сеансовому – передачу даних з тим ступенем надійності, яка їм потрібна. Модель OSI визначає п'ять класів послуг, що надається транспортним рівнем. Ці види послуг відрізняються якістю: терміновістю, можливістю відновлення перерваного зв'язку, наявністю засобів мультиплексування декількох з'єднань між різними прикладними протоколами через загальний транспортний протокол, а головне – здатністю до виявлення і виправлення помилок передачі, таких як спотворення, втрата і дублювання пакетів.

Як правило, всі протоколи, починаючи з транспортного рівня і вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережевих операційних систем (ОС). Як приклад транспортних протоколів можна привести протоколи TCP і UDP стека TCP/IP і протокол SPX стека Novell.

Сеансовий рівень забезпечує управління діалогом для того, щоб фіксувати, яка із сторін є активною, а також надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки замість того, щоб починати все з початку. На практиці небагато програм використовують сеансовий рівень, і він рідко реалізується у вигляді окремих протоколів, хоча функції цього рівня часто об'єднують з функціями прикладного рівня і реалізують в одному протоколі.

Рівень представлення служить для представлення передаваної в мережі інформації, зміст якої при цьому не змінюється. За рахунок рівня представлення інформація, що передається прикладним рівнем однієї системи, завжди буде зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть

подолати синтаксичні відмінності в представленні даних або ж відмінності кодів символів, наприклад кодів ASCII і EBCDIC. На цьому рівні може виконуватися шифрування і дешифрування даних, завдяки якому секретність обміну даними забезпечується відразу для всіх прикладних служб. Прикладом такого протоколу є протокол Secure Socket Layer (SSL), який забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень складає набір різноманітних протоколів, за допомогою яких користувачі мережі отримують доступ до поділюваних ресурсів, а також організують свою спільну роботу за допомогою протоколу електронної пошти. Одиниця даних, якою оперує прикладний рівень, зазвичай називається *повідомленням*.

Існує дуже велика різноманітність служб прикладного рівня. Як приклади протоколів прикладного рівня декілька найбільш поширених реалізацій файлових служб: NCP в операційній системі Novell NetWare, SMB в Microsoft Windows NT, NFS, FTP і TFTP, що входять в стек TCP/IP.

Контрольні запитання

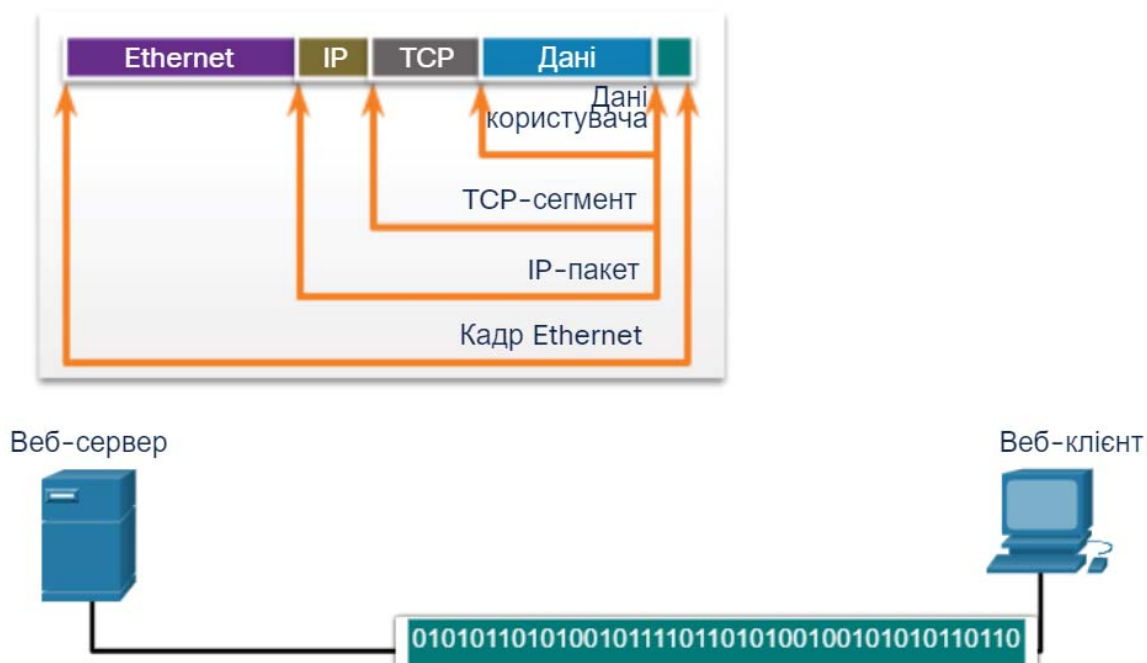
1. Які ключові події в історії розвитку комп'ютерних мереж можна виділити?
2. Які технологічні досягнення сприяли розвитку комп'ютерних мереж?
3. Що таке стандартизація в контексті комп'ютерних мереж і чому вона важлива?
4. Які організації відповідають за стандартизацію комп'ютерних мереж?
5. Які основні стандарти для комп'ютерних мереж існують сьогодні?
6. Які основні організації відомі своєю роботою в області стандартизації комп'ютерних мереж?
7. Які завдання виконують ці організації і як вони впливають на розвиток мережевих технологій?
8. Які приклади стандартів, розроблених цими організаціями, можна навести?
9. Що таке еталонна модель взаємодії відкритих систем і як вона допомагає розуміти роботу комп'ютерних мереж?
10. Назвіть основні рівні в еталонній моделі OSI і поясніть їх функції.

РОЗДІЛ 2. ТЕХНОЛОГІЇ ФІЗИЧНОГО РІВНЯ

Фізичний рівень моделі OSI надає засоби для транспортування бітів, які складають кадр канального рівня, через середовище передавання даних мережі. Цей рівень приймає повний кадр від канального рівня і перетворює його у послідовність сигналів, які передаються у локальне середовище передавання даних. Закодовані біти, що містять кадр, приймаються або кінцевим, або проміжним пристроєм [27].

Під час передачі від вузла джерела до вузла призначення (вузла-адресата) дані піддаються таким перетворенням.

- На транспортному рівні користувачі дані сегментуються, на мережевому - розподіляються по пакетах, а потім інкапсулюються в кадри на канальному рівні.
- Фізичний рівень кодує кадри і формує електричні, оптичні або радіосигнали, за допомогою яких представлена інформація про біти в кожному кадрі.
- Потім ці сигнали послідовно передаються засобами підключення.
- Фізичний рівень вузла призначення приймає ці окремі сигнали від засобів підключення, відновлює представлені ними біти і передає ці біти на канальний рівень у вигляді цілого кадру.



2.1. Середовища передавання даних

Існує три основні типи засобів мережевого підключення. Фізичний рівень створює подання бітів і групує їх для кожного з цих типів таким чином.

– **Мідний кабель:** сигнали являють собою послідовність електричних імпульсів.

– **Оптоволоконний кабель:** сигнали являють собою керовані зміни світлового випромінювання.

– **Бездротова мережа:** сигнали являють собою радіосигнали мікрохвильового діапазону.

Для забезпечення функціональної сумісності на фізичному рівні всі аспекти цих функцій регламентуються організаціями зі стандартизації.

Протоколи і процеси верхніх рівнів моделі OSI виконуються за допомогою програмного забезпечення, розробленого програмістами та вченими-комп'ютерниками. Служби і протоколи в пакеті TCP/IP визначені Інженерною радою Інтернету (IETF, Internet Engineering Task Force).

До фізичного рівня відносять електронні схеми, середовища передавання даних та роз'єми, розроблені інженерами. Тому доречно, щоб стандарти, які регулюють це обладнання, визначались відповідними електротехнічними та комунікаційними інженерними організаціями.

Існує багато різних міжнародних та національних організацій, державних регуляторних організацій, приватних компаній, які займаються створенням і підтримкою стандартів фізичного рівня. Наприклад, стандарти фізичного рівня для апаратного забезпечення, середовищ передавання, кодування та формування сигналів визначаються та регулюються наступними організаціями з питань стандартизації:

- Міжнародна організація зі стандартизації (International Organization for Standardization, ISO)
- Асоціація телекомунікаційної галузі / Асоціація електронної галузі (Telecommunications Industry Association, TIA / Electronic Industries Association, EIA)
- Міжнародний союз електрозв'язку (International Telecommunication Union, ITU)
- Американський інститут національних стандартів (American National Standards Institute, ANSI)
- Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE)

- Національні органи регулювання телекомунікацій, включаючи Федеральну комісію зв'язку (Federal Communication Commission, FCC) в США та Європейський інститут стандартів телекомунікацій (European Telecommunications Standards Institute, ETSI)

Додатково до них, часто існують регіональні групи з питань стандартизації з'єднань, такі як Канадська асоціація стандартизації (Canadian Standards Association, CSA), Європейський комітет з електротехнічної стандартизації (European Committee for Electrotechnical Standardization, CENELEC) і Японська асоціація стандартів (Japanese Standards Association, JSA/JIS), які розробляють локальні специфікації.

Пропускна здатність (bandwidth)

Різні фізичні засоби підключення підтримують різні швидкості передачі бітів. Основними характеристиками передавання даних є пропускна здатність (bandwidth) і продуктивність (throughput).

Пропускна здатність (bandwidth) – це кількісна характеристика, що відображає можливості передавання даних конкретним засобом підключення. У цифрових мережах під пропускну здатністю розуміється обсяг даних, який можна передати з однієї точки в іншу за певний час. Зазвичай пропускну здатність вимірюють у кілобітах на секунду (Кбіт/с), мегабітах на секунду (Мбіт/с) або гігабітах на секунду (Гбіт/с).

Фактична пропускна здатність мережі визначається властивостями фізичних засобів підключення, технологіями передавання та виявлення сигналів у мережі.

На реальну пропускну здатність впливають властивості фізичних засобів підключення, технології, що використовуються, і закони фізики.

Продуктивність

Продуктивність (throughput) – це кількість бітів, що передаються засобами підключення за певний період часу.

Через безліч чинників продуктивність (throughput) зазвичай не відповідає заявленій пропускну здатності (bandwidth) у реалізаціях на фізичному рівні. На продуктивність впливає низка факторів, зокрема такі.

- Обсяг трафіку
- Тип трафіку

– Сумарна затримка, що залежить від кількості мережевих пристроїв між джерелом і пунктом призначення.

Затримки в мережі впливають на підсумковий час, необхідний для доставки даних з однієї точки в іншу.

Продуктивність мережі, що складається з декількох підмереж або декількох сегментів, не може перевищувати швидкість найповільнішого з'єднання між джерелом і одержувачем. Навіть якщо всі або більшість сегментів мають високу пропускну здатність, один-єдиний сегмент із низькою продуктивністю створить вузьке місце, а продуктивність усієї мережі буде знижено.

Існує також третій параметр, що характеризує передачу корисних даних, який називається корисною пропускну здатністю (goodput). Корисна пропускна здатність – це обсяг корисних даних, переданих за певний період часу. Корисна пропускна здатність (goodput) дорівнює продуктивності (throughput) за вирахуванням службового трафіку, необхідного для створення сеансів, підтверджень та інкапсуляції.

Фізичний рівень забезпечує представлення потоку бітів у вигляді змін рівнів напруги, модульованих радіочастотних сигналів або світлових імпульсів. Організаціями зі стандартизації було спільно вироблено вимоги до фізичних, електричних і механічних властивостей засобів підключення для різних видів комунікацій. Ці специфікації гарантують належну роботу кабелів і роз'ємів з різними реалізаціями канального рівня.

2.1.1. Мідний кабель

Характеристики мідного кабелю

Мідні кабелі на сьогоднішній день є найпоширенішими в мережах. Насправді, мідний кабель – це не просто один тип кабелю. Існує три різних типи мідних кабелів, які використовуються в залежності від конкретного випадку.

В мережах використовують мідні носії, оскільки вони є недорогими, легко встановлюються та мають низький електричний опір. Проте, вони характеризуються обмеженою відстанню прокладання та впливом завад на сигнал.

Дані передаються по мідних кабелях у вигляді електричних імпульсів. Детектор в мережному інтерфейсі пристрою призначення повинен отримати такий сигнал, який можна легко декодувати для відновлення відправленого

сигналу. Однак чим більша відстань передання сигналу, тим більші спотворення. Це називається затуханням сигналу. Тому для всіх засобів під'єднання на основі мідних носіїв стандартами встановлено суворі обмеження відстані.

Часові характеристики і значення напруги електричних імпульсів також чутливі до впливу таких двох джерел завад:

- **Електромагнітні завади (ЕМЗ) або радіочастотні завади (РЧЗ)** – сигнали ЕМЗ і РЧЗ можуть спотворювати і погіршувати сигнали даних, що передаються по мідних носіях. Потенційні джерела ЕМЗ і РЧЗ включають радіохвилі і електромагнітні пристрої, такі як люмінесцентні лампи або електричні двигуни.

- **Перехресні завади (crosstalk)** – це перешкоди, при яких електричні або магнітні поля сигналу на одному дроті, впливають на сигнал у суміжних дротах. У телефонних каналах перехресні завади можуть призводити до часткового прослуховування іншої голосової розмови з сусіднього каналу. Зокрема, коли електричний струм протікає по провіднику, він створює навколо нього невелике магнітне поле, яке може впливати на сусідні дроти.

Для протидії негативному впливу ЕМЗ і РЧЗ деякі типи мідних кабелів загорнуті в металеве екранування і потребують належного заземлення.

Щоб протидіяти негативному впливу перехресних завад, в деяких видах мідних кабелів сусідні пари проводів скручені між собою, що ефективно долає вплив таких завад.

Типи мідного кабелю

При створенні мереж використовується три основних типи мідних кабелів (рис. 2.1):

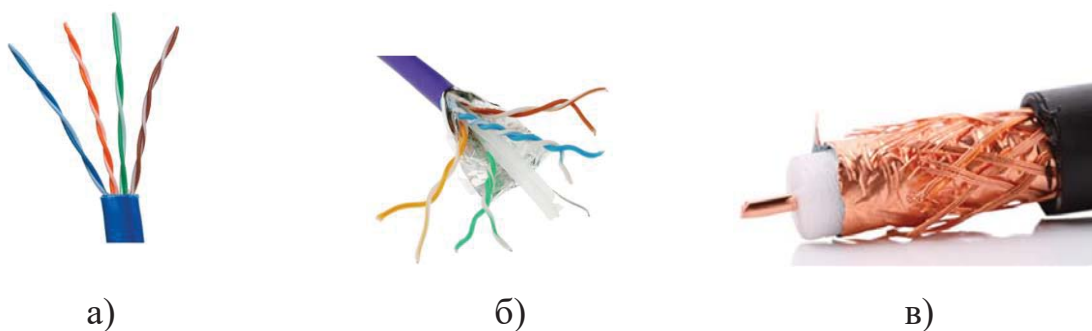


Рис. 2.1. Типи медного кабелю: а) неекранована вита пара (UTP), б) екранована вита пара (STP), в) коаксіальний кабель

Кабель на основі неекранованої витної пари (UTP)

Кабель на основі неекранованої витної пари (UTP) є найпоширенішим засобом під'єднання до мережі. Кабелі UTP з роз'ємами RJ-45 використовуються для з'єднання хостів мережі з проміжними мережними пристроями, такими як комутатори і маршрутизатори.

Кабель UTP для локальних мереж складається з чотирьох пар кольорових дротів, скручених між собою і укладених у гнучку пластикову оболонку, що захищає від незначних фізичних пошкоджень. Скручування дротів захищає від впливу завад від інших дротів.

Кольорове позначення ідентифікує окремі пари і дроти та допомагає в обтисненні кабелю (рис. 2.2). Зовнішня оболонка захищає мідні провідники від фізичних пошкоджень. Попарне перекручування дротів підвищує захист сигналів від завад. Кольорова пластикова ізоляція електрично ізолює дроти один від одного та ідентифікує кожну пару.

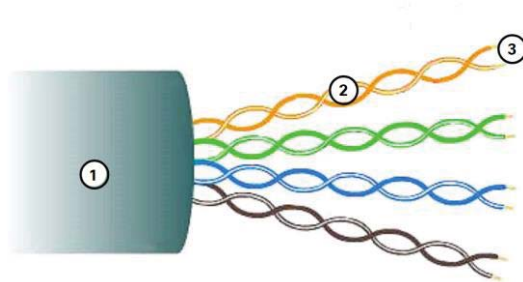


Рис. 2.2. Кабель UTP:

1 – зовнішня оболонка, 2 – попарне перекручування дротів, 3 – кольорова пластикова ізоляція

Кабель на основі екранованої витної пари (STP)

Кабель на основі екранованої витної пари (STP) забезпечує кращий захист від завад, ніж кабель UTP. Однак, в порівнянні з UTP, кабель STP значно дорожчий і складніший в монтажі. Як і для кабелю UTP, з STP використовують роз'єм RJ-45.

В кабелях STP поєднується екранування для захисту від ЕМЗ і РЧЗ та скручування дротів для захисту від перехресних завад. Для підвищення ефективності екранування кабелі STP комплектуються спеціальними екранованими роз'ємами STP. При неправильному заземленні кабелю екран може виступати в ролі антени і приймати небажані сигнали.

Кабель STP використовує чотири пари дротів, кожна з яких загорнута у фольгований екран, які потім всі разом загорнуті у загальне металеве обплетення або фольгу (рис. 2.3).

Коаксіальний кабель

Коаксіальний кабель отримав таку назву тому, що він містить два провідника, які знаходяться на одній осі. Коаксіальний кабель складається з наступних елементів (рис. 2.4):

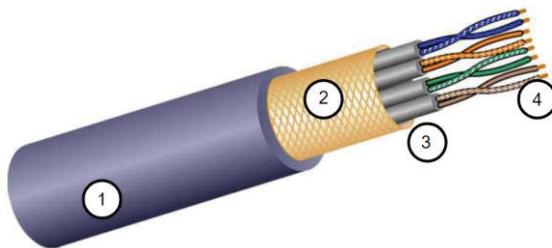


Рис. 2.3. Кабель STP:

1 – зовнішня оболонка, 2 – фольгований або плетений екран, 3 – фольговані екрани, 4 – скручені пари дротів

- Мідний провідник, що використовується для передавання електронних сигналів.
- Шар гнучкої пластикової ізоляції, що оточує мідний провідник.
- Ізоляційний матеріал оточений мідною опліткою або металевою фольгою, яка виконує роль другого дроту в схемі та екрану для внутрішнього провідника. Цей другий шар, або екран, також зменшує кількість зовнішніх електромагнітних завад.
- Зовні кабель покритий кабельною оболонкою для захисту від незначних фізичних пошкоджень.

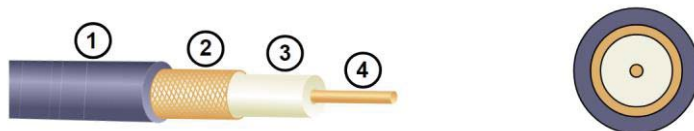


Рис. 2.4. Коаксіальний кабель:

1 – зовнішня оболонка, 2 – плетене мідне екранування, 3 – пластикова ізоляція, 4 – мідний провідник

З коаксіальним кабелем використовують різні типи роз'ємів: конектори байонетного типу Нейла-Консельмана (BNC), типу N та F (рис. 2.5).



Рис. 2.5. Конектори для коаксіального кабелю

Хоча в сучасних мережах Ethernet коаксіальні кабелі фактично поступилися місцем кабелям UTP, однак їх використовують в наступних випадках:

- **Обладнання бездротових мереж** – коаксіальні кабелі приєднують антени до бездротових пристроїв. Коаксіальний кабель забезпечує передання енергії радіосигналу між антенами і радіоапаратурою.
- **Мережі кабельного телебачення з доступом до Інтернету** – провайдери кабельних мереж забезпечують під'єднання до Інтернету для своїх клієнтів шляхом заміни частини коаксіального кабелю і відповідних підсилювальних елементів на волоконно-оптичні кабелі.

Кабель UTP

Властивості кабелю UTP

Кабель на основі неекранованої виткої пари (UTP), що використовується для мережного з'єднання, складається з чотирьох пар скручених мідних дротів з кольоровим маркуванням, укладених в загальну гнучку пластикову оболонку. Завдяки невеликому діаметру кабелю його зручно монтувати.

В кабелях UTP не передбачене екранування для запобігання впливу ЕМЗ і РЧЗ. Замість цього проектувальниками кабелів були знайдені інші способи запобігання негативному впливу перехресних завад:

- *Пригнічення* – проектувальники тепер об'єднують дроти одного електричного кола в пару. Коли два дроти в електричному колі розміщені близько один до одного, їх магнітні поля є протилежними один одному. Таким чином, два магнітних поля компенсують одне одного, а також компенсують будь-які зовнішні впливи ЕМЗ та РЧЗ.
- *Змінна кількість витків у парах дротів* – для підвищення ефекту пригнічення завад проектувальники використовують різний крок для витків у сусідніх парах одного кабелю. Кабелі UTP повинні точно відповідати специфікаціям, які встановлюють допустиму кількість витків на 1 метр (3,28 футів) кабелю. Зверніть увагу, що на рисунку пара дротів

помаранчевий/помаранчево-білий скручена рідше, ніж пара синій/синьо-білий. Пари різних кольорів скручені з різним кроком скрутки.

Стандарти та роз'єми для кабелів UTP

Прокладання кабелю UTP здійснюється згідно стандартів, спільно встановлених організаціями TIA/EIA. Зокрема, стандарт TIA/EIA-568 визначає прокладання кабелів для локальних мереж, у цій сфері найчастіше використовують саме його. Ось деякі з визначених у ньому елементів:

- Типи кабелів
- Довжина кабелів
- Роз'єми
- Обтискання кабелю
- Методи тестування кабелю

Електричні характеристики мідних кабелів визначаються Інститутом інженерів з електротехніки та електроніки (IEEE). IEEE оцінює кабель UTP відповідно до його продуктивності. Кабелі поділяють на категорії, залежно від величини їх пропускну здатності. Наприклад, кабель категорії 5 зазвичай використовують при прокладанні Fast Ethernet специфікації 100BASE-TX. До інших категорій кабелю належать: розширена категорія 5, категорія 6 та категорія 6а.

Кабелі вищих категорій спроектовані та створені для підтримки вищої швидкості передавання даних. По мірі розробки та впровадження нових гігабітних технологій Ethernet, на сьогодні мінімально прийнятним типом кабелю є категорія 5е, а категорія 6 - рекомендований тип для прокладання нових мереж.

На рисунку 2.6 показано три категорії кабелю UTP:

- Категорія 3 спочатку використовувалася для голосового зв'язку по голосових лініях, але пізніше її почали використовувати для передавання даних.
- Категорії 5 і 5е використовуються для передавання даних. Категорія 5 підтримує швидкість 100 Мбіт/с, а категорія 5е - 1000 Мбіт/с.
- Категорія 6 має додатковий роздільник між кожною парою дротів, що дозволяє підтримувати більшу швидкість. Категорія 6 підтримує до 10 Гбіт/с.
- Категорія 7 також підтримує 10 Гбіт/с.
- Категорія 8 підтримує 40 Гбіт/с.

Деякі виробники виготовляють кабелі з покращеними відносно категорії 6а TIA/EIA технічними характеристиками, і їх відносять до категорії 7.

На рисунку 2.6 показана різниця в конструкції між категоріями UTP-кабелю. Категорія 3 з чотирма дротами, категорії 5 та 5е з чотирма витими парами дротів, категорія 6 з чотирма витими парами дротів, де кожна пара має пластиковий роздільник.

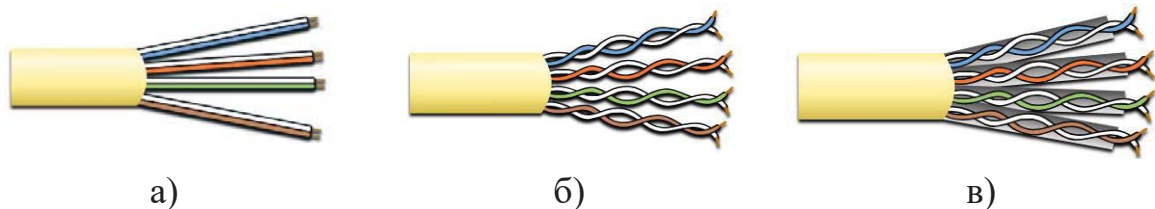


Рис. 2.6. Категорії кабелю UTP:

а) кабель категорії 3 (UTP), б) кабель категорії 5 та 5е (UTP),
в) кабель категорії 6 (STP)

Роз'єм RJ-45 – це конектор, обтиснений на кінці кабелю (рис. 2.7). Гніздовий роз'єм – це розетка на мережному пристрої, стіні або патч-панелі (рис. 2.8).



Рис. 2.7. Штекерний роз'єм RJ-45 для UTP



Рис. 2.8. Гніздовий роз'єм RJ-45 для UTP

UTP-кабель зазвичай має на кінцях роз'єм RJ-45. Стандарт TIA/EIA-568 описує кольорові схеми для приєднання дротів до роз'ємів (pinout) для кабелів Ethernet. UTP-кабель зазвичай має на кінцях роз'єм RJ-45. Стандарт

TIA/EIA-568 описує кольорові схеми для приєднання дротів до роз'ємів (pinout) для кабелів Ethernet.

Прямі та кросоверні кабелі UTP

В різних випадках UTP-кабелі потрібно під'єднувати відповідно до різних схем монтажу. Мається на увазі, що окремі дроти в кабелі можуть бути під'єднані в різному порядку до різних груп контактів у роз'ємах RJ-45.

Основні типи кабелів, які одержуються використанням особливих схем монтажу:

- *Прямий кабель Ethernet (straight-through)* – найпоширеніший тип мережного кабелю. Він зазвичай використовується для з'єднання хоста з комутатором і комутатора з маршрутизатором.

- *Перехресний кабель Ethernet або кросоверний (crossover)* – кабель, що використовується для з'єднання однотипних пристроїв. Наприклад, для з'єднання комутатора з комутатором, хоста з хостом або маршрутизатора з маршрутизатором. Однак перехресні кабелі тепер вважаються застарілими, оскільки NIC використовують кросоверний інтерфейс (auto-MDIX), що залежить від середовища передавання, для автоматичного виявлення типу кабелю та здійснення внутрішнього з'єднання.

Неправильне використання перехресного або прямого кабелю між пристроями не може пошкодити самі пристрої, але з'єднання та зв'язок між ними не відбуватимуться.

На рисунку 2.9 визначено окремі пари дротів для стандартів T568A та T568B.

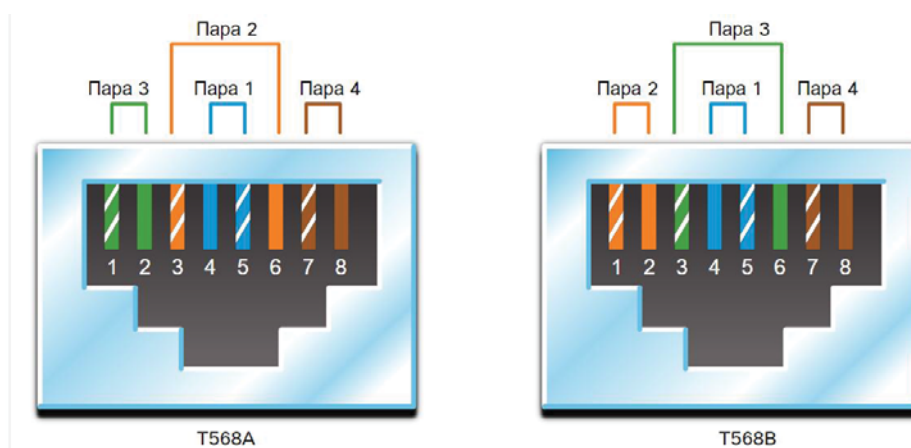


Рис. 2.9. Стандарти T568A та T568B

2.1.2. Волоконно-оптичний кабель

Властивості волоконно-оптичного кабелю

Волоконно-оптичний кабель – це ще один тип кабелю, що використовується в мережах. Через високу вартість, його не так часто застосовують, як різні типи мідного кабелю. Але волоконно-оптичний кабель має певні властивості, які в деяких випадках роблять його найкращим варіантом кабелю.

Волоконно-оптичний кабель передає дані на великі відстані і з більшою пропускною здатністю, аніж будь-які інші мережні носії. На відміну від мідних дротів, оптоволоконний кабель може передавати сигнали з меншим затуханням і забезпечує повну захищеність від ЕМЗ і РЧЗ. Оптоволоконно зазвичай використовується для з'єднання мережних пристроїв.

Оптичне волокно – це гнучка, але надзвичайно тонка прозора нитка з чистого скла, не набагато товща за людську волосину. Для передавання у оптоволоконні біти кодуються у вигляді світлових імпульсів. Оптоволоконний кабель виступає в якості провідника світлових хвиль, або "світловода", для передавання світла між двома кінцями з мінімальними втратами сигналу.

Волоконно-оптичні кабелі традиційно поділяються на два види:

- Одномодове оптоволоконно (SMF, Single-Mode Fiber)
- Багатомодове оптоволоконно (MMF, Multimode Fiber)

Одномодове оптоволоконно (SMF, Single-Mode Fiber)

Основою одномодового оптоволоконна (SMF) є серцевина дуже малого діаметру; для випромінювання світлового променя використовується лазерна технологія (рис. 2.10). SMF широко використовується для організації ліній зв'язку з дальністю у сотні кілометрів, наприклад далекомагістральної телефонії та кабельного телебачення.

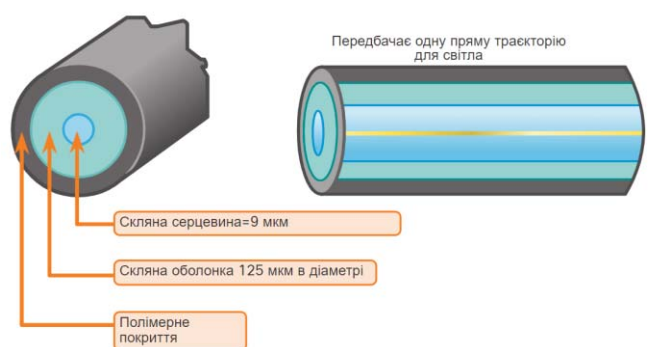


Рис. 2.10. Одномодове оптоволоконно

Багатомодове оптоволокно (MMF, Multimode Fiber)

MMF має більшу серцевину і використовує світлодіодні випромінювачі для надсилання світлових імпульсів. Світло, що випромінюється світлодіодами, потрапляє у багатомодове волокно під різними кутами (рис. 2.11). Такі кабелі популярні у LAN, оскільки дозволяють використовувати недорогі світлодіоди. Багатомодовий кабель забезпечує пропускну здатність до 10 Гбіт/с на відстані до 550 метрів.

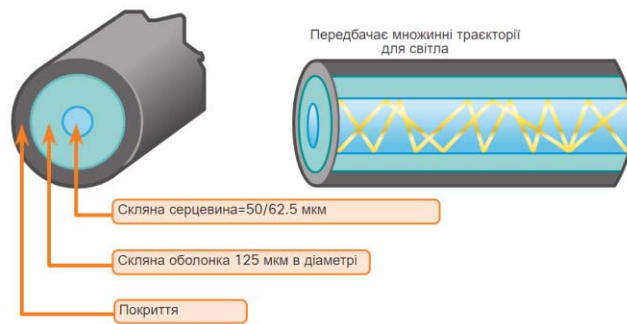


Рис. 2.11. Багатомодове оптоволокно

Однією з основних відмінностей між MMF та SMF є величина розсіювання (дисперсії). Під дисперсією розуміють розсіювання світлового імпульсу з часом. Чим вища дисперсія, тим більші втрати потужності сигналу. MMF має вищу дисперсію, ніж SMF. Тому MMF може передавати лише на 500 метрів без втрати сигналу.

Використання волоконно-оптичного кабелю

Волоконно-оптичні кабелі на сьогодні використовуються в чотирьох галузях:

- *Корпоративні мережі* – використовується для магістральних кабелів і сполучення пристроїв інфраструктури.
- *Волокно до будинку користувача (FTTH, Fiber-to-the-Home)* – використовується для постійного надання широкосмугових послуг для дому та малого бізнесу.
- *Далекомагістральні мережі* – використовується постачальниками послуг для під'єднання країн і міст.
- *Підводні кабельні мережі* – використовується для забезпечення надійних високошвидкісних, високопродуктивних рішень, здатних витримати суворі умови підводного середовища на відстанях аж до трансокеанських. Шукайте в Інтернеті "карта підводної кабельної мережі", щоб переглянути різні он-лайн карти.

Роз'єми для оптоволокна

Оптоволоконний роз'єм (конектор) монтується на кінці оптичного волокна. Використовують різні типи оптоволоконних роз'ємів. Основними відмінностями між типами роз'ємів є розміри і способи механічних з'єднань. Типи конекторів, що будуть використовуватися в мережі, визначаються обладнанням, яке під'єднується.

Донедавна світло в оптоволокні могло рухатись лише в одному напрямку. Для забезпечення повнодуплексного режиму роботи потрібні були два оптоволокна. Тому, у волоконно-оптичних з'єднувальних кабелях є два волокна, на кінцях яких змонтовані стандартні одно-волоконні з'єднувачі. Деякі оптоволоконні з'єднувачі дозволяють під'єднувати як передавальні, так і приймальні волокна. Такі роз'єми називають дуплексними. Стандарти ВХ, наприклад 100BASE-BX, використовують різну довжину хвилі для надсилання та прийому через одне оптоволокно [27].

Волоконно-оптичний патч-корд

Оптоволоконні патч-корди використовують для з'єднання пристроїв інфраструктури. Одномодові та багатомодові патч-корди відрізняють за кольором. Жовтий колір зовнішньої ізоляції використовують для одномодових оптоволоконних кабелів, а помаранчевий (або голубий) – для багатомодових.

2.1.3. Бездротове з'єднання

Властивості бездротового з'єднання

Бездротове з'єднання – це третій спосіб під'єднання до фізичного рівня мережі. Засоби бездротового з'єднання забезпечують передавання двійкових розрядів даних у вигляді електромагнітних сигналів радіочастотного або мікрохвильового діапазону.

З усіх можливих середовищ передавання бездротове з'єднання забезпечує найкращу мобільність, тому кількість під'єднаних пристроїв продовжує збільшуватися. Зараз бездротовий зв'язок є основним способом під'єднання користувачів до домашньої та корпоративної мережі.

Для бездротового зв'язку треба враховувати такі обмеження:

- *Область покриття* – бездротові технології передавання даних добре працюють у відкритому просторі. Однак деякі будівельні матеріали,

що застосовуються при будівництві будівель та споруд, а також місцевий ландшафт можуть обмежувати ефективне покриття.

- *Інтерференція* – бездротовий зв'язок вразливий до завад і може бути спотворений такими поширеними пристроями, як домашні бездротові телефони, деякі види люмінесцентних ламп, мікрохвильові печі та інші бездротові комунікації.

- *Безпека* – покриття бездротового зв'язку не потребує доступу до фізичного носія. Тому пристрої та користувачі, не авторизовані для доступу до мережі, можуть отримати доступ до передавання даних. Мережна безпека є головним компонентом адміністрування бездротової мережі.

- *Спільний доступ до середовища передавання* – WLAN працюють в напівдуплексному режимі, а це означає, що в певний момент часу тільки один пристрій може здійснювати відправлення або отримання. Бездротове середовище передавання є спільним для всіх бездротових користувачів. Велика кількість користувачів, що отримують доступ до WLAN одночасно, призводить до зниження пропускну здатності для кожного користувача.

Типи бездротового з'єднання

Стандарти IEEE та телекомунікаційної галузі для бездротового передавання даних визначають і каналний, і фізичний рівні. У кожному з цих стандартів специфікації фізичного рівня стосуються наступного:

- Перетворення даних у радіосигнали.
- Частоти і потужності передавання.
- Вимог до прийому і декодування сигналу.
- Проектування та конструкції антени.

Стандарти бездротового зв'язку:

- *Wi-Fi (IEEE 802.11)* – технологія бездротової локальної мережі (WLAN), яку зазвичай називають просто Wi-Fi. WLAN використовує протокол на основі зондування носіїв, відомий як множинний доступ з контролем несучої та виявленням колізій (CSMA/CA, Carrier Sense Multiple Access with Collision Detection). Бездротовий NIC перед передаванням повинен спочатку "прослухати" середовище, щоб визначити, чи радіоканал вільний. Якщо передає інший бездротовий пристрій, то NIC повинен зачекати, доки канал не стане вільним. Wi-Fi є торговою маркою Wi-Fi Alliance. Wi-Fi використовується із сертифікованими пристроями WLAN на основі стандартів IEEE 802.11.

- *Bluetooth (IEEE 802.15)* – це стандарт бездротової приватної мережі (WPAN), широко відомий як "Bluetooth". Він використовує процес парування пристроїв для зв'язку на відстані від 1 до 100 метрів.

- *WiMAX (IEEE 802.16)* – загальновідомий як WiMAX (Worldwide Interoperability for Microwave Access), цей бездротовий стандарт використовує топологію точка-багатоточка для забезпечення бездротового широкосмугового доступу.

- *Zigbee (IEEE 802.15.4)* – специфікація, що використовується для низькошвидкісного малопотужного зв'язку. Він призначений для застосунків, які потребують малого діапазону, низької швидкості передавання даних та тривалої роботи акумулятора. Zigbee зазвичай використовується для промислових застосунків та Інтернету-речей (IoT, Internet of Things), таких як бездротові вимикачі світла та збір даних з медичних пристроїв.

Інші бездротові технології, такі як стільниковий та супутниковий зв'язок, також можуть забезпечувати під'єднання до мережі передавання даних.

Бездротова локальна мережа

Загальна реалізація бездротового передавання даних дає змогу пристроям здійснювати бездротове з'єднання через локальну мережу. Загалом, для створення бездротової локальної мережі (WLAN, Wireless LAN) потрібні такі мережні пристрої:

- *Бездротова точка доступу (AP, Access Point)* – вона концентрує бездротові сигнали від користувачів і під'єднується до існуючої інфраструктури на базі мідних кабелів, наприклад, Ethernet. Бездротові маршрутизатори для домашнього та малого бізнесу інтегрують функції маршрутизатора, комутатора та точки доступу в одному пристрої.

- *Бездротові адаптери NIC* – вони надають можливість бездротового зв'язку мережним хостам.

З розвитком технології з'явилася низка стандартів на основі бездротових мереж Ethernet.

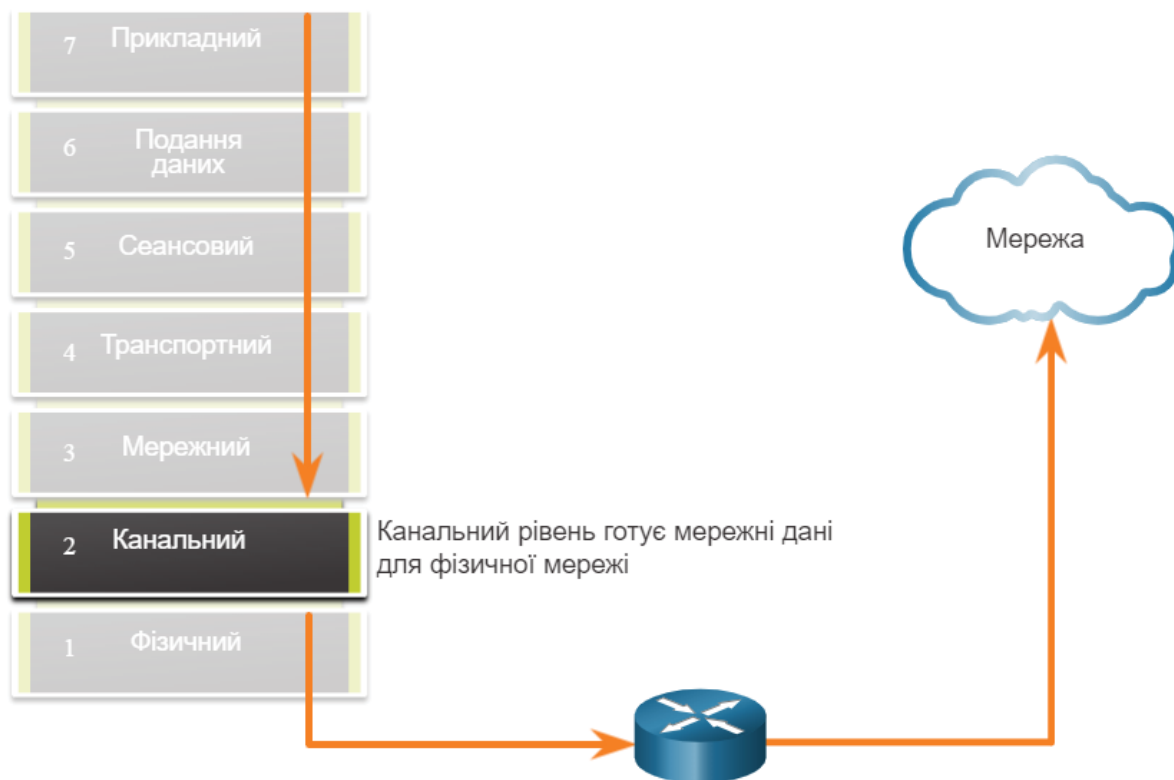
Переваги бездротових технологій передавання даних очевидні, особливо економія на дорогому прокладанні кабелів та зручність мобільності хоста. Мережні адміністратори повинні розробляти та застосовувати сувору політику безпеки та заходи захисту WLAN від несанкціонованого доступу та пошкоджень.

Контрольні запитання

1. Яка основна функція фізичного рівня моделі OSI?
2. Які процеси відбуваються на фізичному рівні під час передачі даних від вузла джерела до вузла призначення?
3. Які три основні типи засобів мережевого підключення і які сигнали вони використовують?
4. Які організації займаються стандартизацією фізичного рівня мережевого обладнання?
5. Які фактори впливають на пропускну здатність (bandwidth) і продуктивність (throughput) мережі?
6. Як вимірюється пропускну здатність і як вона відрізняється від продуктивності?
7. Що таке корисна пропускну здатність (goodput) і як вона обчислюється?
8. Як фізичний рівень забезпечує представлення потоку бітів у мережі?
9. Які переваги мідних кабелів в мережах наведені в тексті?
10. Що таке затухання сигналу і як воно впливає на передачу даних по мідних кабелях?
11. Які два основних джерела завад, вказані в тексті, які можуть впливати на сигнали даних в мідних кабелях?
12. Які заходи приймаються для захисту від негативного впливу електромагнітних завад (ЕМЗ) і радіочастотних завад (РЧЗ) в мідних кабелях?
13. Що таке перехресні завади (crosstalk) і як вони можуть впливати на передачу даних по мідних кабелях?
14. Які два основних типи мідних кабелів згадуються в тексті, і які їх відмінності?
15. Для яких цілей використовується кабель UTP, а для яких - кабель STP?
16. Що таке коаксіальний кабель і які він має елементи?
17. Які основні типи мережних кабелів за схемами монтажу згадуються в тексті, і як вони використовуються?
18. Яким чином розрізняються схеми монтажу T568A та T568B, і як це впливає на підключення мідних кабелів?

РОЗДІЛ 3. ТЕХНОЛОГІЇ КАНАЛЬНОГО РІВНЯ

Канальний рівень моделі OSI (Рівень 2) готує мережні дані для фізичної мережі. Канальний рівень відповідає за зв'язок між мережними інтерфейсними картами (NIC).



Функції канального рівня:

- Забезпечення верхнім рівням можливості отримання доступу до середовища передавання даних. Протокол верхнього рівня не має повної інформації про тип середовища, який використовується для пересилання даних.
- Прийняття даних, зазвичай пакетів Рівня 3 (тобто IPv4 або IPv6), і інкапсуляція їх у кадри Рівня 2.
- Контроль способу розміщення та отримання даних в/з середовища передавання даних.
- Забезпечення обміну кадрами між кінцевими точками через середовище передавання даних.
- Отримання інкапсульованих даних, зазвичай пакетів Рівня 3, і передавання їх відповідному протоколу верхнього рівня.
- Виявлення помилок і відкидання всіх пошкоджених кадрів.

У комп'ютерних мережах хост (вузол) – це пристрій, який може приймати, створювати, зберігати або пересилати дані по каналах комунікації. Вузлом може бути як кінцевий пристрій, такий як ноутбук або мобільний телефон, так і проміжні пристрої, такі як комутатор Ethernet.

Без канального рівня протоколи мережного рівня, такі як IP, мали б передбачати певні заходи для підключення до кожного типу середовища передавання даних, який зустрінеться на шляху доведення. Крім того, кожного разу при розробці нової мережної технології або середовища передавання даних, IP довелося б адаптуватися.

Канальний рівень додає інформацію Рівня 2, Ethernet-адреси NIC призначення та джерела, до пакета Рівня 3. Потім ця інформація конвертується у формат, який підтримується фізичним рівнем (тобто Рівнем 1) (рис. 3.1).



Рис. 3.1. Адреси канального рівня

3.1. Підрівні Канального рівня IEEE 802 LAN/MAN

Стандарти IEEE 802 LAN/MAN характерні для локальних мереж Ethernet, бездротових локальних мереж (WLAN), бездротових персональних мереж (WPAN) та інших типів локальних мереж та мереж мегаполісів. Канальний рівень IEEE 802 LAN/MAN складається з наступних двох підрівнів (рис. 3.2):

- *Logical Link Control (LLC)* – Цей підрівень IEEE 802.2 організовує взаємодію мережного програмного забезпечення верхніх рівнів і апаратного забезпечення пристрою на нижніх рівнях. Він розміщує у кадрі інформацію, що визначає, який протокол мережного рівня використовує цей кадр. Ця інформація дозволяє кільком протоколам Рівня 3, таким як IPv4 і IPv6, використовувати один і той самий мережний інтерфейс і середовище передавання даних.

- *Media Access Control (MAC)* – Реалізує цей підрівень (IEEE 802.3, 802.11 або 802.15) в апаратному забезпеченні. Він відповідає за інкапсуляцію даних і контроль за доступом до середовища передавання даних. Він забезпечує адресацію канального рівня і інтегрується з різними технологіями фізичного рівня.

Підрівень LLC приймає дані мережного протоколу, зазвичай це пакет IPv4 або IPv6, і додає контрольну інформацію Рівня 2, яка допоможе доставити пакет до вузла призначення.

Підрівень MAC керує NIC та іншим обладнанням, яке відповідає за надсилання та отримання даних через дротові або бездротові середовища передавання даних LAN/MAN.

Підрівень MAC також забезпечує контроль доступу до середовища передавання даних, який дозволяє кільком пристроям спілкуватися через загальне (напівдуплексне) середовище передавання даних. Повнодуплексні комунікації не потребують контролю доступу.

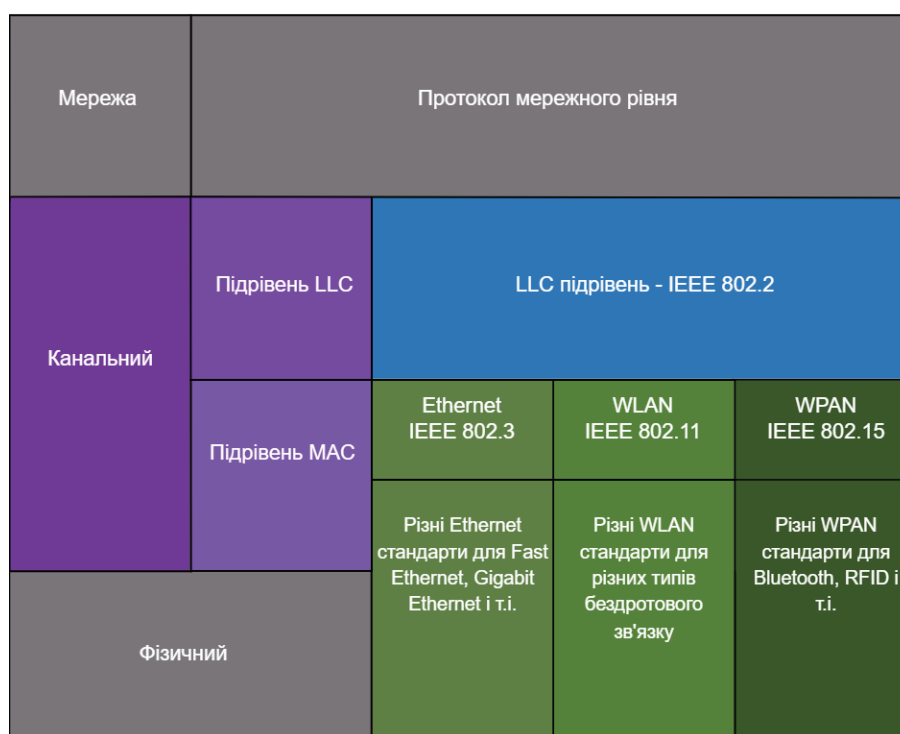


Рис. 3.2. Підрівні (LLC і MAC) канального рівня

Підрівень LLC приймає дані мережного протоколу, зазвичай це пакет IPv4 або IPv6, і додає контрольну інформацію Рівня 2, яка допоможе доставити пакет до вузла призначення.

Підрівень MAC керує NIC та іншим обладнанням, яке відповідає за надсилання та отримання даних через дротові або бездротові середовища передавання даних LAN/MAN.

Підрівень MAC також забезпечує контроль доступу до середовища передавання даних, який дозволяє кільком пристроям спілкуватися через загальне (напівдуплексне) середовище передавання даних. Повнодуплексні комунікації не потребують контролю доступу.

3.2. Стандарти канального рівня

Протоколи канального рівня зазвичай не визначаються документами Request for Comments (RFCs), на відміну від протоколів верхніх рівнів стеку TCP/IP. Інженерна рада Інтернету (Internet Engineering Task Force, IETF) підтримує функціональні протоколи і сервіси стеку протоколів TCP/IP на верхніх рівнях, але вона не визначає функції і роботу рівня мережного доступу стеку TCP/IP.

Наступні інженерні організації визначають відкриті стандарти і протоколи рівня мережного доступу (тобто фізичного і канального рівнів моделі OSI):

- Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE)
- Міжнародний союз електрозв'язку (International Telecommunication Union, ITU)
- Міжнародна організація зі стандартизації (International Organization for Standardization, ISO)
- Американський інститут національних стандартів (American National Standards Institute, ANSI)

3.3. Фізичні та логічні топології

Топологія мережі – це розташування мережних пристроїв та зв'язки між ними. Існує два типи топологій, які використовуються при описі LAN і WAN мереж:

- *Фізична топологія* – Визначає фізичні з'єднання та як кінцеві та проміжні пристрої (такі як маршрутизатори, комутатори та точки бездротового доступу) зв'язані між собою. Топологія може також містити конкретне розташування пристрою, наприклад номер кімнати і місце розташування на стійці обладнання.

- *Логічна топологія* – Стосується того, яким шляхом мережа передає кадри від одного вузла до іншого. Ця топологія визначає віртуальні з'єднання, враховуючи інтерфейси пристроїв і схеми IP-адресації Рівня 3.

Канальний рівень "бачить" логічну топологію мережі, коли контролює доступ до середовища передавання даних. Логічна топологія впливає на механізм створення кадрів (framing) та тип керування доступом до середовища передавання даних.

3.3.1. Топології WAN

Зазвичай WAN взаємозв'язані за допомогою трьох загальних фізичних топологій WAN.

Топологія точка-точка

Фізичні топології точка-точка безпосередньо з'єднують два вузли (рис. 3.3). При такому розташуванні два вузли не ділять середовище передавання даних з іншими вузлами. Крім того, при використанні протоколу послідовного зв'язку, наприклад, Point-to-Point Protocol (PPP), вузлу не потрібно визначати, чи призначений вхідний кадр тому чи іншому вузлу. Тому протоколи канального рівня можуть бути дуже простими, оскільки всі кадри у середовищі передавання даних можуть іти тільки до або з одного з цих двох вузлів. Вузол розміщує кадри до середовища передавання даних на одному кінці і ці кадри виймаються з середовища передавання даних вузлом на іншому кінці схеми точка-точка.



Рис. 3.3. Топологія «Точка-точка»

Hub and spoke

Це WAN версія топології зірка, в якій центральний пристрій зв'язує між собою пристрої філіалів за допомогою з'єднання точка-точка. Пристрої філіалів не можуть обмінюватися даними одне з одним без участі центрального пристрою (рис. 3.4).

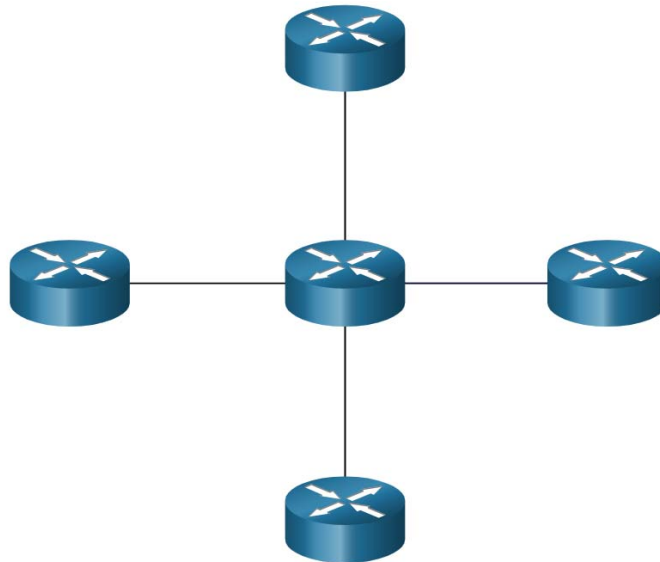


Рис. 3.4. Топологія «Hub and spoke»

Повнозв'язна топологія

Ця топологія забезпечує високу доступність, але вимагає щоб кожна кінцева система була з'єднана з кожною іншою системою. Тому адміністративні та фізичні витрати можуть бути значними. Кожен канал по суті є з'єднанням "точка-точка" з іншим вузлом (рис. 3.5).

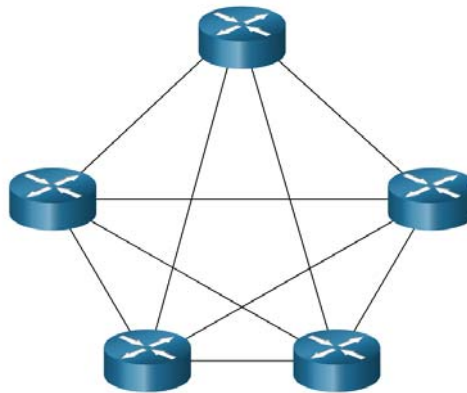


Рис. 3.5. Повнозв'язна топологія

3.3.2. Топології LAN

В локальних мережах множинного доступу кінцеві пристрої (тобто вузли) з'єднані між собою за допомогою топологій "зірка" або "розширена зірка" (рис. 3.6). У цьому типі топології кінцеві пристрої під'єднуються до центрального проміжного пристрою, в даному випадку – до комутатору Ethernet.

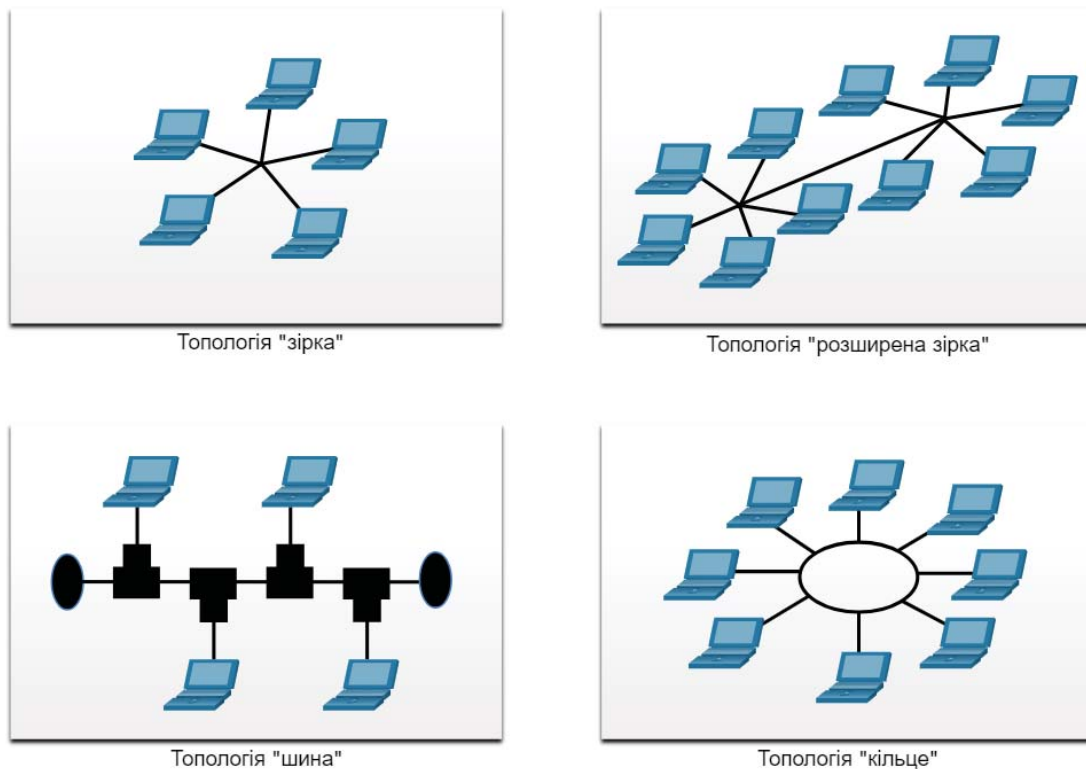


Рис. 3.6. Фізичні топології

Розширена зірка розширює цю топологію підключенням декількох комутаторів Ethernet. Для топологій "зірка" та "розширена зірка" характерна простота монтажу, вони дуже масштабовані (легко додавати та видаляти кінцеві пристрої), і дозволяють легко знайти та усунути несправність. Ранні зіркові топології з'єднували кінцеві пристрої з використанням концентраторів Ethernet.

Іноді ми маємо тільки два пристрої, з'єднані в локальній мережі Ethernet. Наприклад – два з'єднані між собою маршрутизатори. Це є прикладом використання топології точка-точка в Ethernet [27].

3.3.3 Застарілі LAN топології

Ранні варіанти Ethernet і застаріла Token Ring технології LAN використовували два інших типи топологій:

- *Шина* – Всі кінцеві системи з'єднані одна з одною в ланцюг і на кожному кінці ланцюг завершується у певній формі. Проміжні пристрої, такі як комутатори, не обов'язково з'єднуються з кінцевими пристроями. В минулому мережі Ethernet часто будувались за топологією "шина" з використанням коаксіальних кабелів через низьку ціну і простоту налаштування.

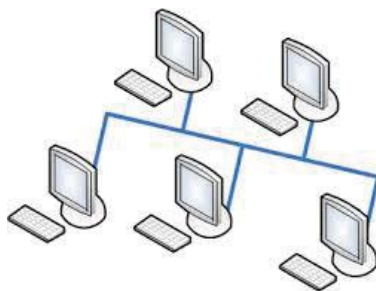


Рис. 3.7. Топологія «Шина»

- *Кільце* – Кінцеві системи підключені до відповідних сусідів, утворюючи кільце. На відміну від топології шини, для кільця не потрібно виконувати термінування. Топологія "кільце" використовувалась в застарілих мережах Fiber Distributed Data Interface (FDDI) та Token Ring.

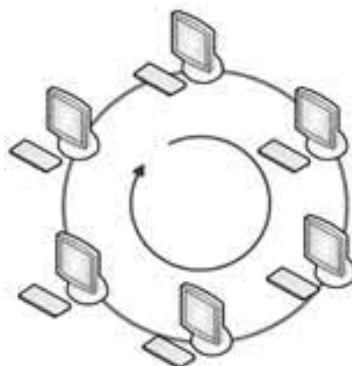


Рис. 3.8. Топологія «Кільце»

3.3.4. Напівдуплексний та повнодуплексний зв'язок

Існує два поширених режими дуплексу.

Напівдуплексний зв'язок

Обидва пристрої можуть передавати і приймати в середовищі передавання даних, але не можуть робити це одночасно. WLAN і застарілі топології типу "шина" з концентраторами Ethernet використовують напівдуплексний режим. Напівдуплексний режим дозволяє лише одному пристрою надсилати або отримувати одночасно дані в середовищі з множинним доступом.

Повнодуплексний зв'язок

Обидва пристрої можуть одночасно передавати і приймати в середовищі передавання даних. Канальний рівень передбачає, що середовище передавання даних доступне для передачі обом вузлам в будь-

який час. Комутатори Ethernet працюють у режимі повного дуплексу за замовчуванням, але вони можуть працювати і в напівдуплексному режимі, якщо підключаються до такого пристрою, як концентратор Ethernet.

3.3.5. Методи контролю доступу

Мережі Ethernet і WLAN є прикладами мереж множинного доступу. Мережа множинного доступу – це мережа, що може мати два або більше кінцевих пристроїв, які намагаються отримати доступ до мережі одночасно.

Деякі мережі множинного доступу вимагають правил, щоб керувати тим, як пристрої поділяють доступ до середовища передавання даних. Існує два основних методи контролю доступу для середовищ множинного доступу:

- Конкурентний доступ
- Контрольований доступ

Конкурентний доступ

В мережах множинного доступу з конкурентним доступом, всі вузли працюють в напівдуплексному режимі, конкуруючи за використання середовища передавання даних. Однак лише один пристрій може надіслати дані одночасно. Таким чином, потрібна процедура вирішення проблеми, коли одночасно передають більше ніж один пристрій. Прикладами методів конкурентного доступу є:

- Множинний доступ з контролем несучої та виявленням колізій (CSMA/CD), що використовується в застарілих LAN Ethernet з топологією "шина"
- Множинний доступ з контролем несучої і униканням колізій (CSMA/CA), що використовується в бездротових локальних мережах

Контрольований доступ

В мережі множинного доступу з контрольованим доступом кожен вузол має свій власний час для використання середовища передавання даних. Ці детерміновані типи застарілих мереж є неефективними, оскільки пристрій повинен чекати своєї черги, щоб отримати доступ до середовища передавання даних. Прикладами мереж множинного доступу з контрольованим доступом є:

- Застарілий Token Ring
- Застарілий ARCNET

Конкурентний доступ – CSMA/CD

Прикладами мереж з конкурентним доступом є:

- Бездротова локальна мережа (використовує CSMA/CA)
- Застаріла Ethernet LAN з топологією "шина" (використовує CSMA/CD)
- Застаріла Ethernet LAN з використанням концентратора (використовує CSMA/CD)

Ці мережі працюють у напівдуплексному режимі, тобто лише один пристрій може надсилати або отримувати дані одночасно. Це потребує процесу, який визначає, коли пристрій може надсилати дані, і що відбувається, коли кілька пристроїв надсилають дані одночасно.

Якщо одночасно передають два пристрої, відбудеться колізія. Для застарілих локальних мереж Ethernet обидва пристрої виявлять наявність колізії в мережі. Це частина скорочення CSMA/CD – виявлення колізій (CD). NIC порівнює передані дані з отриманими, або визначає, що амплітуда сигналу вище норми в середовищі передавання даних. Дані, відправлені обома пристроями, будуть пошкоджені і їх потрібно переслати повторно.

Конкурентний доступ з уникненням конфліктів – CSMA/CA

Інша форма CSMA, яка використовується у IEEE 802.11 WLAN, – це множинний доступ з прослуховуванням несучої/униканням колізій (CSMA/CA).

CSMA/CA використовує метод, подібний до CSMA/CD, щоб визначити, чи є чистим середовище передавання даних. CSMA/CA використовує додаткові методи. У бездротових середовищах пристрій не може виявити наявність колізії. CSMA/CA не виявляє колізій, але намагається їх уникнути, чекаючи перед передаванням. Кожен пристрій, який передає, зазначає тривалість часу, яка йому потрібна для цієї пересилки. Всі інші бездротові пристрої отримують цю інформацію і знають, як довго середовище передавання даних буде недоступним.

3.3.6. Кадр

Канальний рівень готує інкапсульовані дані (зазвичай пакет IPv4 або IPv6) для транспортування через локальне середовище передавання даних, додаючи до них заголовки і трейлер, щоб створити кадр.

Протокол канального рівня відповідає за зв'язок між інтерфейсними мережними картами (NIC-to-NIC) в одній мережі. Хоча існує багато різних

протоколів канального рівня, які описують кадри канального рівня, кожен тип кадру має три основні частини:

- Заголовок
- Дані
- Трейлер

На відміну від інших протоколів, які виконують інкапсуляцію, канальний рівень додає інформацію у вигляді трейлера в кінці кадру.

Всі протоколи канального рівня інкапсулюють дані в полі даних кадру. Однак структура кадру і поля, що містяться в заголовку і в трейлері, залежать від конкретного протоколу.

Немає жодної структури кадру, яка б відповідала потребам транспортування всіх видів даних по всіх типах середовища передавання даних. Залежно від середовища кількість контрольної інформації, необхідної у кадрі, змінюється відповідно до вимог контролю доступу до середовища передавання даних та логічної топології. Наприклад, WLAN-кадр повинен містити процедури уникання колізій і тому вимагає додаткової контрольної інформації порівняно з Ethernet-кадром.

Поля кадру

Механізм створення кадрів (framing) розбиває потік на групи, придатні для розшифровки, при цьому контрольна інформація додається до заголовку і до трейлеру, у вигляді значень в різних полях. Цей формат забезпечує структуру фізичних сигналів, яка розпізнається вузлами і декодується в пакети на вузлі призначення.

Основні поля кадру показані на рисунку 3.9. Не всі протоколи включають всі ці поля до кадру. Стандарти для певного протоколу канального рівня визначають фактичний формат кадру.



Рис. 3.9. Основні поля кадру.

Кадр містить наступні поля:

- *Прапори початку та завершення кадру* – використовуються для визначення меж початку та кінця кадру.
- *Адресація* – Вказуються вузли джерела та призначення в середовищі передавання даних.
- *Тип* – Визначає протокол Рівня 3, дані якого розташовані в полі даних.
- *Керування* – Визначає спеціальні служби контролю потоку, такі як якість обслуговування (QoS). QoS надає пріоритет пересилання повідомленням певного типу. Наприклад, кадри передачі голосу поверх IP (VoIP) зазвичай отримують пріоритет, через їх чутливість до затримки.
- *Дані* – Містить корисне навантаження кадру (тобто заголовок пакета, заголовок сегмента та дані).
- *Виявлення помилок* – Розташовано після даних для формування трейлера.

Протоколи канального рівня додають трейлер в кінці кожного кадру. В процесі, який називається виявленням помилок, трейлер дозволяє визначити чи прийшов кадр без помилок. Логічна або математична сума бітів кадру розміщується в трейлері. Канальний рівень додає виявлення помилок, оскільки сигнали в середовищі передавання даних можуть потрапити під дію інтерференції, бути спотворені або втрачені, що суттєво змінить значення бітів, представлених цими сигналами.

Вузол, що передає, створює логічну суму вмісту кадру, відому як циклічні надлишкові перевірки (CRC). Це значення розміщується в полі контрольної послідовності кадру (frame check sequence, FCS). В Ethernet-кадрі FCS забезпечує вузлу-отримувачу можливість визначити, чи були помилки під час передачі кадру.

3.3.7. Адреси Рівня 2

Канальний рівень забезпечує адресацію, яка використовується для транспортування кадру через спільне середовище передавання даних. Адреси пристроїв на цьому рівні називають фізичними адресами. Адресація канального рівня міститься в заголовку кадру і визначає вузол призначення кадру в локальній мережі. Це поле зазвичай знаходиться на початку кадру, тому NIC може швидко визначити, чи відповідає адреса призначення його власній адресі Рівня 2, перш ніж приймати решту кадру. Заголовок кадру також може містити адресу джерела кадру.

На відміну від логічних адрес Рівня 3, які є ієрархічними, фізичні адреси не вказують, в якій мережі знаходиться пристрій. Фізична адреса є унікальною для конкретного пристрою. Пристрій все одно працюватиме з тією ж фізичною адресою Рівня 2, навіть якщо його перемістити до іншої мережі або підмережі. Таким чином, адреси Рівня 2 використовуються тільки для підключення пристроїв до одного спільного середовища передавання даних, в одній IP-мережі.

Кадри LAN та WAN

Протоколи Ethernet використовуються дротовими локальними мережами. Бездротові комунікації підпадають під протоколи WLAN (IEEE 802.11). Ці протоколи були розроблені для мереж множинного доступу.

WAN традиційно використовують інші типи протоколів для різних типів топологій точка-точка, hub-spoke та повнозв'язна. Протягом багатьох років поширеними WAN-протоколами були:

- Point-to-Point Protocol, PPP (Протокол точка-точка)
- High-Level Data Link Control (HDLC)
- Frame Relay
- Asynchronous Transfer Mode (ATM)
- X.25

Ці протоколи Рівня 2 зараз замінюються в WAN на Ethernet.

В мережі TCP/IP всі протоколи Рівня 2 OSI працюють з IP на Рівні 3 моделі OSI. Однак те, який використовується протокол Рівня 2, залежить від логічної топології та фізичного носія.

Кожен протокол виконує керування доступом до середовища передавання даних для конкретних логічних топологій Рівня 2. Це означає, що різні мережні пристрої можуть виступати в якості вузлів, які працюють на каналному рівні при реалізації цих протоколів. Цими пристроями є NIC на комп'ютерах, а також інтерфейси маршрутизаторів і комутаторів Рівня 2.

Протокол Рівня 2, який використовується для певної топології мережі визначається технологією, яка використовується для реалізації цієї топології. Яка технологія використовується, визначається розміром мережі, в термінах кількості хостів і географічного охоплення, а також послуг, які надаватимуться мережею.

LAN зазвичай використовує технологію високої пропускної здатності, яка може підтримувати велику кількість хостів. Відносно невелика географічна область локальної мережі (одна будівля або кампус з декількох

будівель) і висока щільність користувачів роблять цю технологію рентабельною [8].

Однак використання технології високої пропускної здатності зазвичай не є економічно вигідним для WAN, які охоплюють великі географічні області (наприклад, місто або декілька міст). Вартість фізичних каналів великої довжини і технологія, що використовується для передачі сигналів на ці відстані, як правило, призводять до зниження пропускної здатності.

Різниця в пропускній здатності зазвичай призводить до використання різних протоколів для LAN і WAN.

До протоколів канального рівня належать:

- Ethernet
- 802.11 Wireless
- Point-to-Point Protocol, PPP (Протокол точка-точка)
- High-Level Data Link Control (HDLC)
- Frame Relay

Контрольні запитання

1. Які функції виконує канальний рівень мережі?
2. Що визначає підрівень Logical Link Control (LLC) в стандартах IEEE 802 LAN/MAN?
3. Яка різниця між фізичною та логічною топологією мережі?
4. Назвіть три типи топологій WAN та надайте короткий опис кожного з них.
5. Які інженерні організації визначають стандарти і протоколи рівня мережного доступу?
6. Які два поширені режими дуплексу використовуються в мережах?
7. Які основні характеристики напівдуплексного режиму зв'язку?
8. Що означає повнодуплексний зв'язок і які пристрої часто використовують його?
9. Які два основних методи контролю доступу в мережах множинного доступу?
10. Які приклади методів конкурентного доступу в мережах множинного доступу?
11. Які приклади мереж множинного доступу з контрольованим доступом?

12. Які основні поля кадру на канальному рівні і як вони використовуються?

13. Що таке фізичні адреси на канальному рівні і як вони використовуються?

14. Які типи протоколів канального рівня використовуються в бездротових локальних мережах (WLAN)?

15. Які типи протоколів канального рівня традиційно використовуються в бездротових мережах?

РОЗДІЛ 4. ОСНОВНІ СТАНДАРТИ КОМП'ЮТЕРНИХ МЕРЕЖ

4.1. Технологія Ethernet (802.3)

Найбільше поширення серед стандартних мереж одержала мережа *Ethernet* [17; 26; 43]. Вперше вона з'явилася в 1972 році (розроблювач фірма Xerox). Мережа виявилася досить вдалою, і внаслідок цього її в 1980 році підтримали такі найбільші компанії, як DEC і Intel (об'єднання цих компаній назвали DIX за першими буквами їхніх назв). Їх стараннями в 1985 році мережа *Ethernet* стала міжнародним стандартом, її прийняли найбільші міжнародні організації по стандартах: комітет 802 IEEE (Institute of Electrical and Electronic Engineers) і ECMA (European Computer Manufacturers Association).

Стандарт одержав назву IEEE 802.3 ("eight oh two dot three"). Він визначає множинний доступ до моноканального типу шини з виявленням конфліктів і контролем передачі, тобто із уже згадуваним методом доступу CSMA/CD. Цьому стандарту задовольняли й деякі інші мережі, тому що рівень його деталізації невисокий. В результаті мережі стандарту IEEE 802.3 нерідко були несумісні між собою як за конструктивними, так і за електричними характеристиками. Однак останнім часом стандарт IEEE 802.3 вважається стандартом саме мережі *Ethernet*.

Основні характеристики первісного стандарту IEEE 802.3:

- топологія – шина;
- середовище передачі – коаксіальний кабель;
- швидкість передачі – 10 Мбіт/с;
- максимальна довжина мережі – 5 км;
- максимальна кількість абонентів – до 1024;
- довжина сегмента мережі – до 500 м;
- кількість абонентів на одному сегменті – до 100;
- метод доступу – CSMA/CD;
- вузькополосна передача, тобто без модуляції (моноканал).

Мережа *Ethernet* зараз найбільш популярна у світі (більше 90% ринку). Цьому в чималому ступені сприяло те, що із самого початку характеристики, параметри, протоколи мережі були відкриті, у результаті чого величезне число виробників в усьому світі стали випускати апаратуру *Ethernet*, повністю сумісну між собою.

В класичній мережі *Ethernet* застосовувався 50-омний коаксіальний кабель двох видів (товстий і тонкий). Однак останнім часом (з початку 90-х років) найбільше поширення одержала версія *Ethernet*, що використовує як *середовище передачі* виту пару. Визначений також стандарт для застосування в мережі оптоволоконого кабелю. Для обліку цих змін у стандарт IEEE 802.3 були зроблені відповідні додавання. В 1995 році з'явився додатковий стандарт на більш швидку версію *Ethernet*, що працює на швидкості 100 Мбіт/с (так званий *Fast Ethernet*, стандарт IEEE 802.3u), що використовує як *середовище передачі* виту пару або оптоволоконний кабель. В 1997 році з'явилася версія на швидкість 1000 Мбіт/с (*Gigabit Ethernet*, стандарт IEEE 802.3z). З 2002 року з'явився стандарт *10 Gigabit Ethernet*, також відомий як *10GbE*. Він визначає версію *Ethernet* з номінальною швидкістю передачі даних 10 Гбіт/с, що є в 10 разів швидше за *Gigabit Ethernet*. Стандарт для оптоволокна специфікований в IEEE 802.3-2005, а для скрученої пари в IEEE 802.3an-2006. *40 Gigabit Ethernet* або *40GbE*, а також *100 Gigabit Ethernet*, або *100GbE* – стандарти *Ethernet*, що розроблялися IEEE P802.3ba *Ethernet Task Force* з початку листопада 2007 року та були остаточно прийняті в червні 2010. Ці стандарти підтримують передачу *Ethernet* пакетів на швидкості 40 та 100 Гбіт/с крізь декілька окремих 10 Гбіт/с або 25 Гбіт/с ліній.

Крім стандартної топології шина усе ширше застосовуються топології типу пасивна зірка й пасивне дерево. При цьому передбачається використання репітерів і репітерних концентраторів, що з'єднують між собою різні частини (сегменти) мережі. В результаті може сформуватися деревоподібна структура на сегментах різних типів (рис. 4.1).

Як сегмент (частина мережі) може виступати класична шина або одиничний абонент. Для шинних сегментів використовується коаксіальний кабель, а для променів пасивної зірки (для приєднання до концентратора одиночних комп'ютерів) – вита пара та оптоволоконний кабель. Головна вимога до отриманої в результаті топології – щоб у ній не було замкнутих шляхів (петель). Фактично виходить, що всі абоненти з'єднані у фізичну шину, тому що сигнал від кожного з них поширюється відразу в усі сторони і не вертається назад (як у кільці).

Максимальна довжина кабелю мережі в цілому (максимальний шлях сигналу) теоретично може досягати 6,5 км, але практично не перевищує 3,5 км. В мережі *Fast Ethernet* не передбачена фізична топологія шина, використовується тільки пасивна зірка або пасивне дерево. До того ж в *Fast Ethernet* набагато жорсткі вимоги до граничної довжини мережі. Адже при

збільшенні в 10 разів швидкості передачі й збереженні формату пакета його мінімальна довжина стає в десять разів коротше. У такий спосіб в 10 разів зменшується припустима величина подвійного часу проходження сигналу по мережі (5,12 мкс проти 51,2 мкс в Ethernet). Для передачі інформації в мережі Ethernet застосовується стандартний манчестерський код.

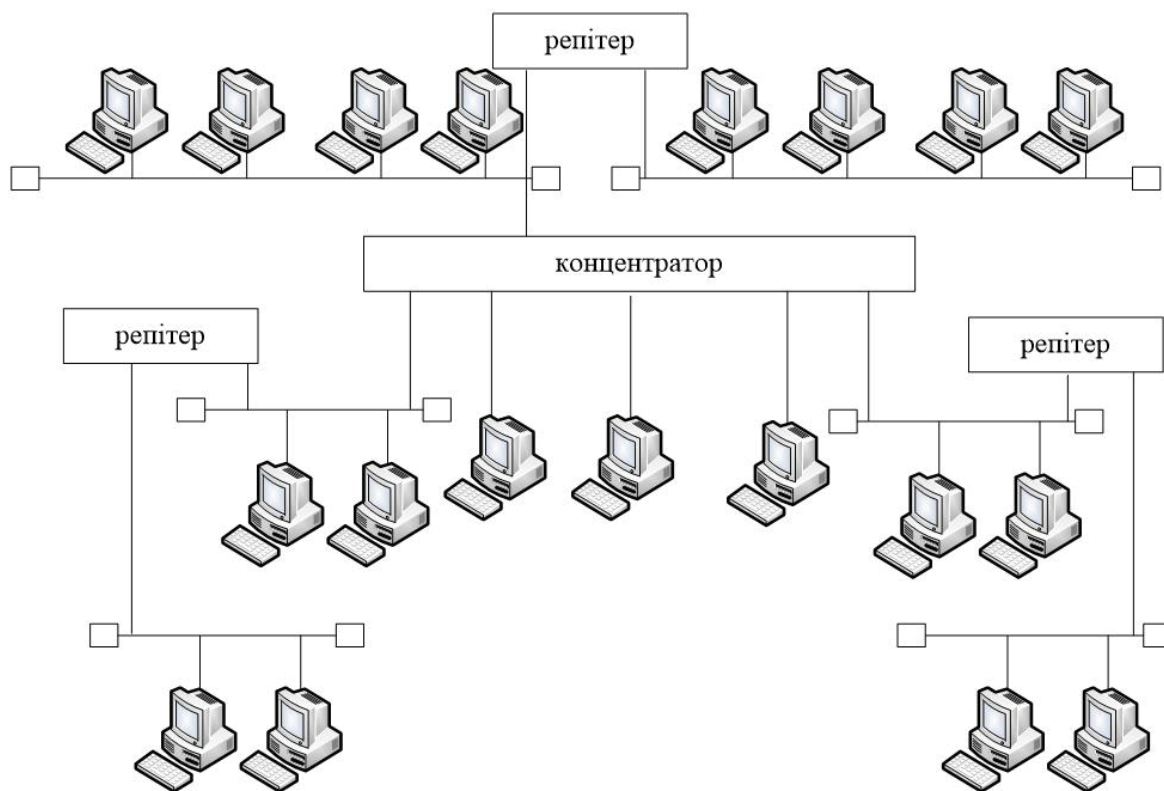


Рис. 4.1. Класична топологія мережі Ethernet

4.1.1. Метод доступу CSMA/CD

Всі існуючі стандарти сімейства Ethernet (Fast Ethernet, Gigabit Ethernet) використовують один і той же метод розділення середовища передачі даних – CSMA/CD.

CSMA/CD – метод колективного доступу з розпізнаванням несучої і виявленням колізій (Carrier Sense Multiply Access with Collision Detection). Початковою топологією, стандартів Ethernet була топологія загальна шина (рис. 4.2).

Цей метод застосовується виключно в мережах із загальною шиною. Всі комп'ютери такої мережі мають безпосередній доступ до загального

середовища. Одночасно всі комп'ютери мережі мають можливість одержати дані, які будь-який з комп'ютерів почав передавати на загальну шину. Середовище, до якого підключені всі комп'ютери, працює в режимі колективного доступу (Multiply Access, MA). Саме завдяки простоті схеми підключення стандарти сімейства Ethernet є дуже популярними.

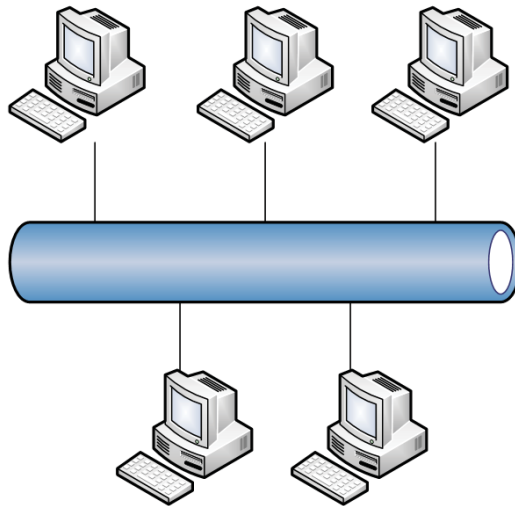


Рис. 4.2. Топологія загальна шина

Всі дані, що передаються по мережі, поміщаються в *кадри* – інформаційні блоки канального рівня, що мають встановлену структуру (формат). У заголовку кадру обов'язково вказується унікальна адреса комп'ютера-одержувача.

Щоб передавати кадр, комп'ютер-відправник повинен переконатися, що фізичне середовище вільне. Це досягається прослуховуванням основної гармоніки сигналу, яка також називається несучою частотою (*carrier sense, CS*). Ознакою незайнятості середовища є відсутність на ній несучої частоти, яка при манчестерському способі кодування дорівнює 5 – 10 МГц, залежно від послідовності одиниць і нулів, що передаються в даний момент.

Якщо середовище вільне, то комп'ютер-одержувач починає передачу кадру. Вся решта комп'ютерів, підключених до кабелю, може розпізнати факт передачі кадру, але приймає його той комп'ютер, який дізнається власну адресу в заголовку кадру. Потім комп'ютер-одержувач записує вміст прийнятого кадру в свій внутрішній буфер, обробляє одержані дані, передає їх вгору по своєму стеку, а потім посилає по кабелю кадр-відповідь. Адреса комп'ютера-відправника міститься в початковому кадрі, тому комп'ютер-одержувач знає, кому потрібно передати відповідь.

Після закінчення передачі кадру всі вузли мережі зобов'язані витримати технологічну паузу в 9,6 мкс – міжкадровий інтервал, яка необхідна для приведення мережевих адаптерів в початковий стан, а також для запобігання монопольному захопленню середовища однією станцією.

Не виключені ситуації, коли дві або більше станцій одночасно вирішують, що середовище вільне, і намагаються передати свої кадри даних по загальному середовищу. Це можливо навіть, не дивлячись на реалізацію механізму прослуховування середовища і наявність паузи між передачею кадрів. При цьому відбувається *колізія (collision)* – явище, при якому вміст двох кадрів накладається в загальному середовищі і відбувається спотворення інформації.

Всі комп'ютери одночасно спостерігають за переданими по фізичному середовищу сигналами. Якщо передані і спостережувані сигнали відрізняються, то фіксується виявлення колізії (*collision detection, CD*). Комп'ютер, що виявив колізію, перериває передачу свого кадру і підсилює ситуацію колізії посилкою в мережу спеціальної послідовності з 32 біт, званою *jam-послідовністю*. Після цього комп'ютер-відправник, що виявив колізію, зобов'язаний припинити передачу і зробити паузу протягом короткого випадкового інтервалу часу. Випадкова пауза Π вибирається за формулою:

$$\Pi = L \times I_g,$$

де I_g – інтервал відстрочки, який дорівнює 512 бітових інтервалів; L – натуральне число, обране з рівною ймовірністю з діапазону $[0; 2^N]$.

Випадкова пауза може приймати значення від 0 до 52,4 мс.

У даній формулі інтервал відстрочення виражений в бітових інтервалах.

Бітовий інтервал (bt) рівний часу між появою двох послідовних біт даних. Для швидкості 10 Мбіт/с величина бітового інтервалу дорівнює 0,1 мкс.

Якщо 16 послідовних спроб передачі кадру викликають колізію, то передавач повинен припинити спроби і відкинути цей кадр.

Чітке розпізнавання колізій всіма станціями мережі є необхідною умовою коректної роботи мережі Ethernet. Для надійного розпізнавання колізій повинне виконуватися наступне співвідношення:

$$T_{\min} \geq PDV,$$

де $T_{\min}$ – час передачі кадру мінімальної довжини, PDV – час, за який сигнал колізії встигає розповсюдитися до найдалшого вузла мережі. Оскільки у гіршому разі сигнал повинен пройти двічі між найбільш віддаленими один від одного станціями мережі (в один бік проходить неспотворений сигнал, а в обратному напрямку розповсюджується вже спотворений колізією сигнал), цей час називається *часом подвійного обороту (Path Delay Value, PDV)*.

При виконанні цієї умови станція, що передає, повинна встигати виявити колізію, яку викликав переданий її кадр, ще до того, як вона закінчить передачу цього кадру. Очевидно, що виконання цієї умови залежить, з одного боку, від довжини мінімального кадру і пропускної здатності мережі, а з іншого боку, від довжини кабельної системи мережі і швидкості розповсюдження сигналу в кабелі (для різних типів кабелю ця швидкість дещо відрізняється).

Всі параметри протоколу Ethernet (стандарт 802.3) підібрані так, щоб при нормальній роботі вузлів мережі колізії завжди чітко розпізнавалися.

4.1.2. Формати кадрів технології Ethernet

В мережі використовуються кадри змінної довжини зі структурою, представленої на рис. 4.3. (цифри показують кількість байт)



Рис. 4.3. Структура кадру мережі Ethernet

Довжина кадру Ethernet (тобто пакета без преамбули) повинна бути не менш 512 бітових інтервалів або 51,2 мкс (саме така гранична величина подвійного часу проходження в мережі). Передбачено індивідуальну, групову й широкомовну адресацію.

У кадр Ethernet входять наступні поля:

- *Преамбула* складається з 8 байт, перші сім являють собою код 10101010, а останній байт – код 10101011. У стандарті IEEE 802.3 восьмий байт називається ознакою початку кадру (SFD – Start of Frame Delimiter) і утворює окреме поле пакета.

- *Адреси одержувача (приймача) і відправника (передавача)* включають по 6 байт і будуються за стандартами. Ці адресні поля обробляються апаратурою абонентів.

- *Поле керування (L/T – Length/Type)* містить інформацію про довжину поля даних. Воно може також визначати тип використовуваного протоколу. Прийнято вважати, що якщо значення цього поля не більше 1500, то воно вказує на довжину поля даних. Якщо ж його значення більше 1500, то воно визначає тип кадру. Поле керування обробляється програмно.

- *Поле даних* повинне містити в собі від 46 до 1500 байт даних. Якщо пакет повинен містити менш 46 байт даних, то поле даних доповнюється байтами заповнення. Відповідно до стандарту IEEE 802.3, у структурі кадру виділяється спеціальне поле заповнення (pad data – незначні дані), що може мати нульову довжину, коли даних досить (більше 46 байт).

- *Поле контрольної суми (FCS – Frame Check Sequence)* містить 32-розрядну циклічну контрольну суму кадру (CRC) і служить для перевірки правильності передачі кадру.

Таким чином, мінімальна довжина кадру (пакета без преамбули) становить 64 байта (512 біт). Саме ця величина визначає максимально припустиму подвійну затримку поширення сигналу по мережі в 512 бітових інтервалів (51,2 мкс для Ethernet або 5,12 мкс для Fast Ethernet). Стандарт припускає, що преамбула може зменшуватися при проходженні пакета через різні мережні пристрої, тому вона не враховується. Максимальна довжина кадру дорівнює 1518 байтам (12144 біта, тобто 1214,4 мкс для Ethernet, 121,44 мкс для Fast Ethernet). Це важливо для вибору розміру буферної пам'яті мережного обладнання й для оцінки загальної завантаженості мережі [9].

4.1.3. Специфікації фізичного середовища Ethernet

Ethernet працює на Канальному та Фізичному рівнях. Це сімейство мережних технологій, які визначені в стандартах IEEE 802.2 та 802.3. Ethernet підтримує пропускну здатність каналу:

10 Мбіт/с

100 Мбіт/с

1000 Мбіт/с (1 Гбіт/с)

10 000 Мбіт/с (10 Гбіт/с)

40 000 Мбіт/с (40 Гбіт/с)

100 000 Мбіт/с (100 Гбіт/с)

Для мережі Ethernet, що працює на швидкості 10 Мбіт/с, стандарт визначає чотири основних типи сегментів мережі, орієнтованих на різні середовища передачі інформації:

10BASE5 (товстий коаксіальний кабель);

10BASE2 (тонкий коаксіальний кабель);

10 BASE-T (вита пара);

10 BASE-FL (оптоволоконний кабель).

Найменування сегмента містить у собі три елементи: цифра “10” означає швидкість передачі 10 Мбіт/с, слово BASE – передачу в основній смузі частот (тобто без модуляції високочастотного сигналу), а останній елемент – припустиму довжину сегмента: “5” – 500 метрів, “2” – 200 м (точніше, 185 м) або тип лінії зв'язку : “Т” – вита пара (від англійського “twisted-pair”), “F” – оптоволоконний кабель (від англійського “fiber optic”).

Точно так само для мережі Ethernet, що працює на швидкості 100 Мбіт/с (*Fast Ethernet*) стандарт визначає три типи сегментів, що відрізняються типами середовища передачі:

100 BASE-T4 (зчетверена вита пара);

100 BASE-TX (здвоєна вита пара);

100 BASE-FX (оптоволоконний кабель).

Тут цифра “100” означає швидкість передачі 100 Мбіт/с, буква “Т” – виту пару, буква “F” – оптоволоконний кабель. Типи 100 BASE-TX і 100 BASE-FX іноді поєднують під ім'ям 100 BASE-X, а 100 BASE-T4 і 100 BASE-TX – під ім'ям 100 BASE-T.

Gigabit Ethernet (GbE) – термін, що описує набір технологій для передавання пакетів Ethernet зі швидкістю 1 Гбіт/с. Він визначений у документі IEEE 802.3-2005.

1000BASE-TX (UTP/STP cat 6,7)

1000BASE-LX10 (оптоволоконний кабель)

1000BASE-BX10 (оптоволоконний кабель)

1000BASE-EX (оптоволоконний кабель)

1000BASE-ZX (оптоволоконний кабель)

10 *Gigabit Ethernet* або 10GbE був найновішим (на 2006 рік) і найшвидшим з існуючих стандартів Ethernet. Він визначає версію Ethernet з

номінальною швидкістю передавання даних 10 Гбіт/с, що в 10 разів швидше за Gigabit Ethernet. Стандарт для оптоволокна специфікований в IEEE 802.3-2005, а для крученої пари в IEEE 802.3an-2006.

10GBASE-CX4 (мідний кабель CX4)

10GBASE-T (UTP/STP cat 6,6a,7)

10GBASE-LRM (оптоволоконний)

10GBASE-KX4 (для з'єднальної плати)

10GBASE-PR (оптоволоконний)

40-gigabit Ethernet (або 40GbE) і *100-gigabit Ethernet* (або 100GbE) – стандарти Ethernet, розроблені групою IEEE P802.3ba Ethernet Task Force у період з 2007 по 2011 рік. Ці стандарти є наступним етапом розвитку групи стандартів Ethernet, що мали до 2010 року найбільшу швидкість у 10 гігабіт/с. У нових стандартах забезпечується швидкість передавання даних у 40 і 100 гігабіт на секунду.

40GBase-KR4 (для з'єднальної плати)

100GBase-KP4 (для з'єднальної плати)

100GBase-KR4 (для покращеної з'єднальної плати)

40GBase-CR4 (мідний біаксіальний кабель)

100GBase-CR10 (мідний біаксіальний кабель)

40GBase-T (UTP cat 8) (оптоволоконний)

40GBase-SR4 (оптоволоконний)

100GBase-SR10 (оптоволоконний)

100GBase-ER4 (оптоволоконний)

40GBase-FR (оптоволоконний)

Стандарт 10Base-2

Стандартний фізичний інтерфейс 10Base-2 складається з твердого дроту розташованого в центрі кабелю, обгорнутого ізоляцією. Навколо ізоляції розташований циліндричний провідник (мідна сітка). Зовнішній провідник покритий захисною оболонкою. Вид кабелю наведений на рис.4.4.

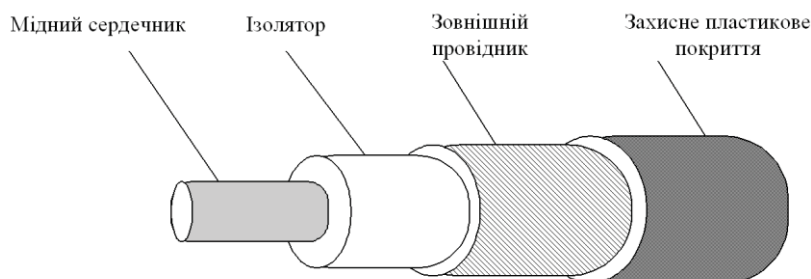


Рис. 4.4. Вид кабелю стандарту 10Base-2

Завдяки своїй конструкції коаксіальні кабелі володіють високою пропускну здатністю і відмінною завадостійкістю. Пропускна здатність залежить від довжини кабелю. Для кабелю довжиною в 1 км досягає швидкість передачі від 1 до 2 Гбіт/с. Можуть також використовуватись і більшої довжини, однак з меншою швидкістю передачі, або з проміжними підсилювачами. Зазвичай використовуються два типа кабелів: 50-омний для передачі цифрових даних і 75-омний для передачі аналогової інформації.

Широкополосні коаксіальні кабелі в основному використовуються для передачі аналогових сигналів. Це прототип аналогових телефонних ліній зі смугою більш ніж 4 КГц, є з'єднувальними лініями у комп'ютерній мережі, яка використовує аналогову передачу. Специфікація 10Base-2 визначає наступні параметри: 10 визначає частоту несучого коливання (10 МГц), яке розповсюджується через середовище, Base – визначає основний принцип доступу до фізичного середовища – це метод CSMA/CD і 2 визначає товщину кабелю – 2 дюйми (тонкий коаксіал).

Топологію сегмента мережі стандарту 10Base-2 наведено на рис. 4.5.

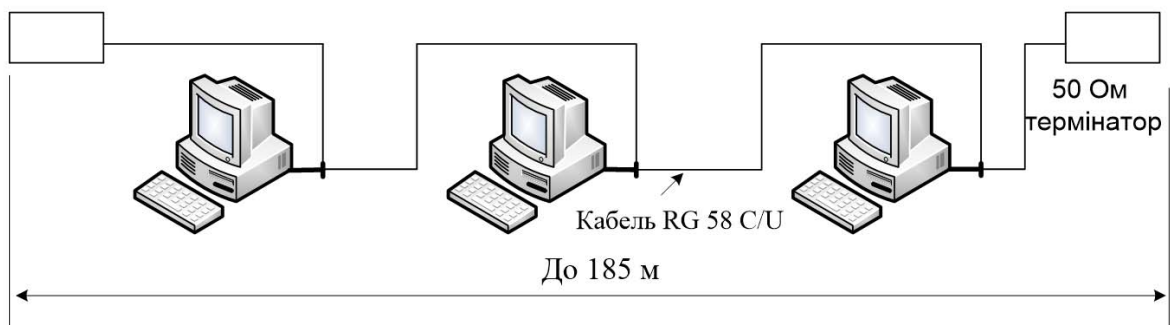


Рис. 4.5. Мережа стандарту 10Base-2

Реалізація цього стандарту на практиці приводить до найбільш простого рішення для кабельної мережі, тому що для з'єднання комп'ютерів потрібні тільки мережні адаптери й Т-конектори. Однак цей вид кабельних з'єднань найбільше сильно підданий аваріям і збоям: кабель сприйнятливий до завад, у моноканалі є велика кількість механічних з'єднань (кожний Т-конектор дає три механічних з'єднання, два з яких мають життєво важливе значення для всієї мережі), користувачі мають доступ до з'єднувачів і можуть порушити цілісність моноканалу. Крім того, естетика і ергономічність цього рішення залишають бажати кращого, тому що від кожної станції через Т-конектор відходять два досить помітних дроти, які під столом часто утворюють моток кабелю – запас, необхідний на випадок навіть невеликого переміщення робочого місця.

Стандарт 10Base-5

Специфікація 10Base-5 відрізняється від 10Base-2 тільки товщиною кабелю, він є більш жорстким, тому використовувався в основному на прямих ділянках кабельної системи.

Кабель використовується як моноканал для всіх станцій. Сегмент кабелю має максимальну довжину 500 м (без повторювачів) і повинен мати на кінцях термінатори, опором 50 Ом, що поглинають сигнали, що поширюються за допомогою кабелю, і завадостійкістю при виникненні відбитих сигналів.

Різні компоненти мережі, виконаної на товстому коаксіалі, показані на рис. 4.6.

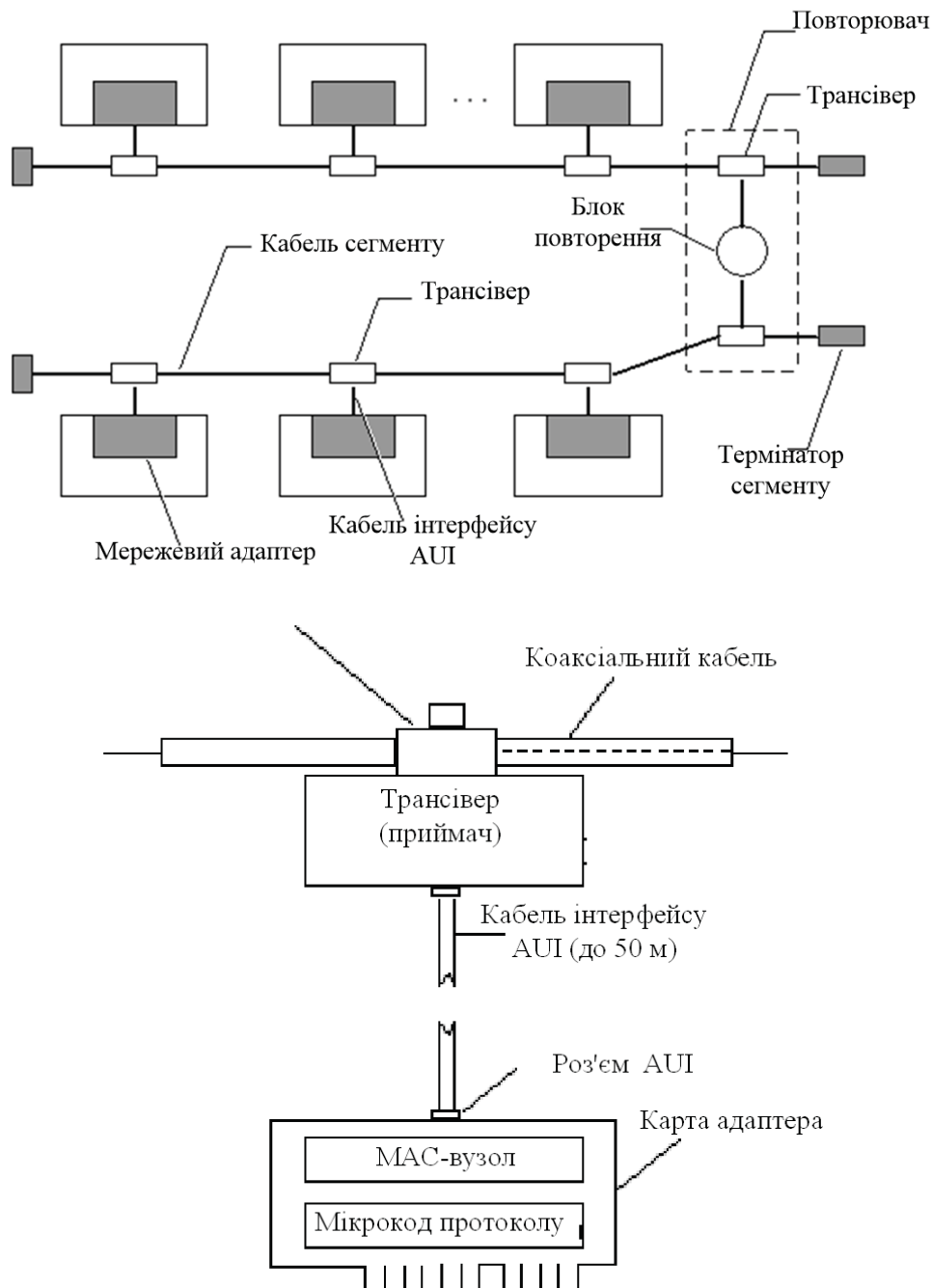


Рис. 4.6. Компоненти фізичного рівня мережі стандарту 10 Base-5, що складається із двох сегментів

Станція повинна підключатися до кабелю за допомогою приймача – трансівера. Трансівер встановлюється безпосередньо на кабелі та підпитується від мережного адаптера комп'ютера.

Трансівер може приєднуватися до кабелю як методом проколювання, що забезпечує безпосередній фізичний контакт, так і безконтактним методом.

Трансівер з'єднується з мережним адаптером інтерфейсним кабелем AUI (Attachment Unit Interface) довжиною до 50 м, що складається з 4 витих пар (адаптер повинен мати роз'єм AUI). Допускається підключення до одного сегмента не більше 100 трансіверів, причому відстань між підключеннями трансіверів не повинне бути менше 2,5 м.

Трансівер – це частина мережного адаптера, що виконує наступні функції: прийом і передача даних з кабелю на кабель, визначення колізій на кабелі, електрична розв'язка між кабелем і іншою частиною адаптера, захист кабелю від некоректної роботи адаптера.

До достоїнств стандарту 10Base-5 відносяться:

- гарна захищеність кабелю від зовнішніх впливів,
- порівняно велика відстань між вузлами,
- можливість простого переміщення робочої станції в межах довжини кабелю AUI.

До недоліків варто віднести:

- високу вартість кабелю;
- складність його прокладки;
- наявність спеціального інструмента для закладення кабелю;
- при пошкодженні кабелю або поганому з'єднанні відбувається збій роботи всієї мережі;
- необхідно заздалегідь передбачити підводку кабелю до всіх можливих місць установки комп'ютерів.

Загальним недоліком стандартів 10Base-5 і 10Base-2 є відсутність оперативної інформації про стан моноканалу. Пошкодження кабелю виявляється відразу ж (мережа перестає працювати), але для пошуку відрізка, що відмовив, кабелю необхідний спеціальний прилад – кабельний тестер.

Стандарт 10Base-T

Вита пара складається з двох ізольованих мідних дротів, як правило, діаметром 1 мм. Скручування дротів по спіралі дозволяє запобігати

випромінюванню електромагнітних хвиль кабелем подібно антені. Іншими словами пару дротів інтерферували. Першим застосуванням витой пари є телефонна мережа. Вита пара дозволяє передавати сигнал без підсилення на відстані в декілька км, на більш великі відстані необхідно використовувати повторювачі, підсилювачі, комутатори. Вита пара може використовуватись для передачі як аналогових так і цифрових сигналів. Смуга пропускання залежить від діаметра і довжини дротів. Висока швидкість (декілька Мбіт/с) може бути досягнута на відстанях в декілька км. Вита пара дозволяє отримати користувачам задовільне відношення якості каналу/пропускна смуга каналу, що істотно конкурує з такими типами кабелю як коаксіал, оптоволокно та інші види.

Вита пара може бути 5 категорій, дві з яких використовуються для побудови локальних обчислювальних мереж.

Cat 3 – вита пара категорії 3 складається з чотирьох пар з двома ізолюваними дротами звитими друг з другом. Чотири такі пари звичайно розміщуються в пластиковій оболонки і дозволяли підключати 4 простих телефонних апарата або два багатоканальних. На зміну витой пари cat 3 прийшла вита пара cat 5, яка відрізняється від cat 3 більшою кількістю витків на 1 см довжини та тефлоновою ізоляцією, що надає менше наводок та кращу якість передачі сигналу на великі відстані.

Ethernet кабелі можуть розділитися на багато типів, як-от Cat5, Cat5e, Cat 6, Cat 7, Cat 8 тощо. Для високошвидкісних додатків впроваджено такі Ethernet кабелі з ширшою пропускною спроможністю, як кабель Cat 6, кабель Cat 6a і Cat 7 кабелі.

Кабель Cat5e та Cat6

Cat5e і Cat6 кабелі використовуються для передавання цифрової та аналогової інформації. Але Cat5e найчастіше зустрічається в наявних кабельних системах. Cat5e широко використовується для побутових і комерційних Ethernet-кабелів. Cat5e також є найбільш гнучким для укладання на поворотах і кутах. Ця категорія може обробляти перенесення даних зі швидкістю 1000 Мбіт/с і підходить для технології Gigabit Ethernet. А Cat6 кабель пропонує швидкість до 10GBASE-T або 10-Gigabit Ethernet, тому що Cat 6 кабель має високу пропускну здатність. Кабелі Cat6 розраховані на робочі частоти до 250 МГц, а категорії 5e тільки до 100 МГц. Вита пара категорії 6 передбачає більш суворі вимоги до перехресних перешкод, а також системного шуму. Cat6 забезпечує кращу продуктивність мережі. При швидкості передачі 1 Гбіт/с

Cat5e має більше сенсу. У разі запиту меншого шуму, менших помилок і високої швидкості передавання даних виберіть Cat6 кабель.

Кабель Cat6 та Cat6a

Cat6 та Cat6a: очевидно, що 10GbE Cat 6a кабель має кращу мережеву продуктивність, ніж 10GbE Cat6 кабель. Кабель Cat6a 10GBASE-T з використанням роз'єму RJ45 може забезпечувати продуктивність 10G з більш високими частотами (500MHz) і більш довгими лініями зв'язку (100m), в порівнянні з кабелем Cat6 (250MHz, 55m). Порівняно з Cat6, Cat6a кабель має міцнішу оболонку, яка зменшує міжкабельні наведення і покращує відношення сигнал/шум.

Кабель Cat7

Фактично стандарт Cat7 був ратифікований для підтримки 10Gbps на 100m раніше, ніж Cat6a кабель. Основною перевагою кабелю Cat7 є те, що він забезпечує екранування для кожної з чотирьох пар дротів і для чотирьох пар загалом. Тож Cat7 кабель має кращу завадостійкість. Але навпаки, екранування робить Cat7 кабель менш гнучким і керованим. Ключовими проблемами є те, що пари дротів повинні бути повністю оточені екраном у кабелі від кінця до кінця, і повинні забезпечувати належне заземлення.

Кабель Cat8

Під час порівняння Cat7 і Cat8, частота передавання і довжина кабелю також мають важливе значення. Cat7 кабель забезпечує продуктивність до 600MHz, а Cat8 кабель до 2000MHz. Максимальна довжина кабелю Cat7 становить 100m з 10Gbps, а Cat8 - 30m з 25Gbps або 40 Gbps.

Вита пара може бути двох типів: UTP (unshided twisted pair) – неекранована вита пара (рис. 4.7) і STP (shided twisted pair) – екранована вита пара (рис. 4.8). З точки зору захищеності від наведень і промислових завад краще використовувати STP – кабель, однак якщо в межах корпорації або замкнутих приміщенні не має необхідності використовувати екрановану пару, то UTP – кабель є більш зручним для прокладення і експлуатації.

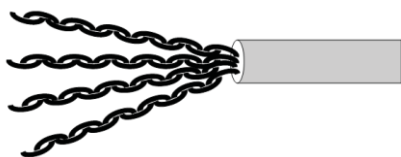


Рис. 4.7. UTP 3 категорії



Рис. 4.8. STP 3 категорії

Стандарт визначає бітову швидкість передачі даних 10 Мб/с і максимальну відстань відрізка виті пари між двома безпосередньо зв'язаними вузлами (станціями й концентраторами) не більше 100 м при використанні виті пари якості не нижче категорії 3.

Можливо ієрархічне з'єднання концентраторів у дерево (рис. 4.9). Для забезпечення синхронізації станцій при реалізації процедур доступу CSMA/CD і надійного розпізнавання станціями колізій у стандарті визначене максимальне число концентраторів між будь-якими двома станціями мережі.

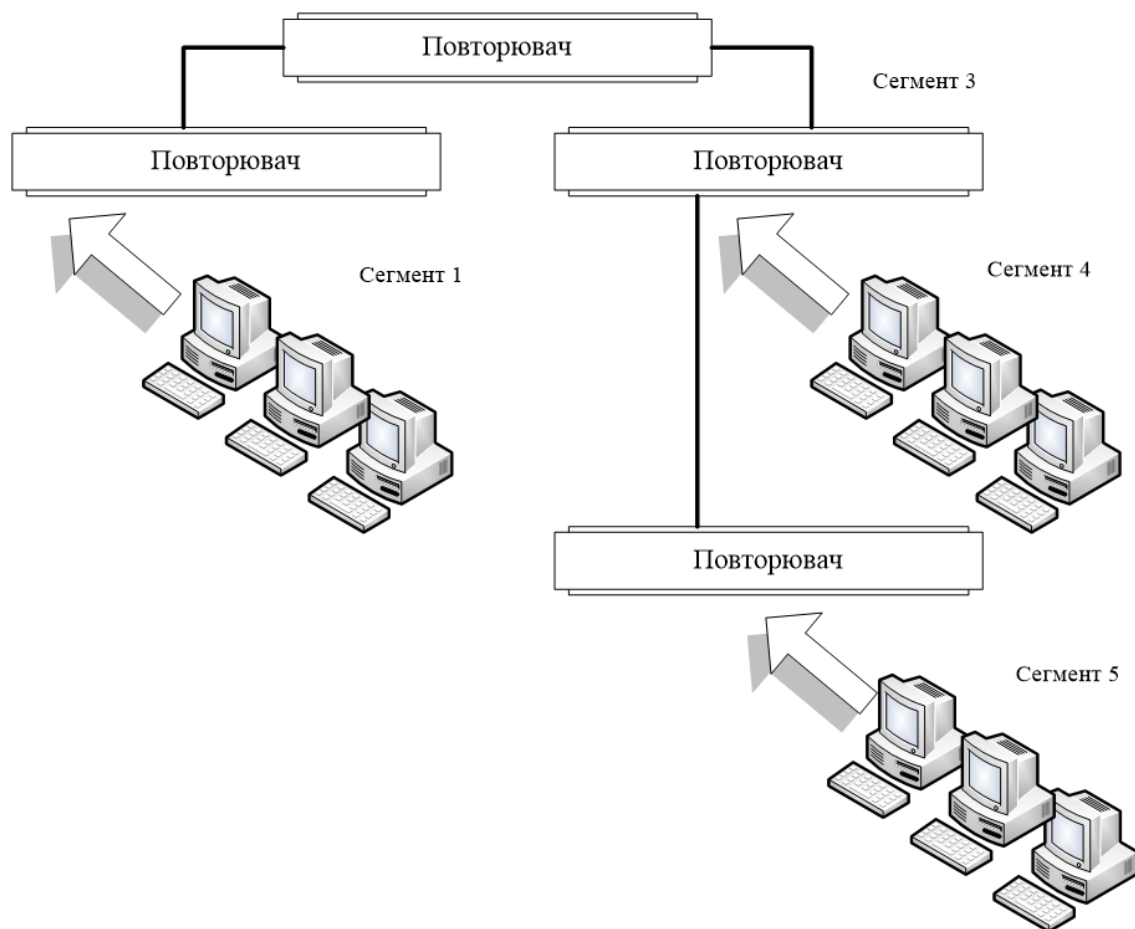


Рис. 4.9. Повторювачі (концентратори)

Загальна кількість станцій в мережі 10 Base-T не повинна перевищувати 1024.

Мережі, побудовані на основі стандарту 10 Base-T, володіють у порівнянні з коаксіальними варіантами Ethernet'а багатьма перевагами. Ці переваги пов'язані з поділом загального фізичного кабелю на окремі кабельні відрізки, підключені до центрального комунікаційного пристрою. І хоча логічно ці відрізки утворять загальний домен колізій, їх фізичний поділ

дозволяє контролювати їх стан і відключати у випадку обриву, короткого замикання або несправності мережного адаптера на індивідуальній основі. Це обставина істотно полегшує експлуатацію більших мереж Ethernet, тому що концентратор звичайно автоматично виконує такі функції, повідомляючи при цьому адміністратора мережі про виниклу проблему.

10 Base FL/SL

Оптоволоконний Ethernet є найбільш прогресивним фізичним середовищем, яке дозволяє задовольняти постійно зростаючим вимогам телекомунікаційних технологій сучасності. Світло є найбільш швидкісним переносником енергії на великі відстані, тому цей тип фізичного середовища використовується для передачі сигналів практично в усіх високошвидкісних технологіях (FDDI, ATM, Gigabit Ethernet і інші).

Існує декілька типів оптоволоконного кабелю.

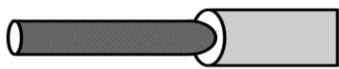


Рис. 4.10. Одномодове волокно

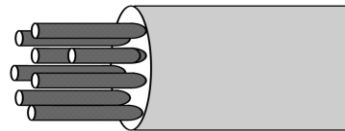


Рис. 4.11. Багатомодове волокно

Фізичний рівень 100Base-FX

100BaseFX – версія для оптоволокна з довжиною хвилі 1300 нм [7; 9; 17; 26; 43]. Логічно близька до *100BaseTX* – те ж логічне кодування 4В/5В. У напівдуплексі дальність 412 м – обмеження за часом подвійного обороту. У повному дуплексі дальність визначається властивістю волокна: може досягати від 2 до 32 км.

100BaseSX – новий стандарт на дешевих короткохвильових (830 нм) світлодіодних передавачах і багатомодовому волокні. Дальність зв'язку обмежена волокном і менше, ніж у FX, – всього 300 м, зате підтримується сумісність з *10BaseFL* і автоматичне узгодження швидкості передачі 10/100 Мбіт/с.

Фізичний рівень 100Base-TX

100BaseTX – найбільш популярна версія Fast Ethernet, що використовує дві виті пари категорії 5 (рис. 4.12). За використання з'єднувачів повністю відповідає *10BaseT*. Можлива робота в напівдуплексному і повнодуплексному режимах. Логічне кодування виробляється по схемі 4В/5В – 4 біта початкової інформації перетворюються в 5-бітовий символ. Надмірність використовується для підвищення достовірності і службових цілей.

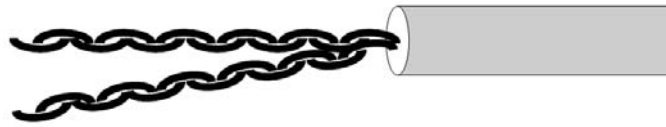


Рис. 4.12. Витя пара категорії 5

Фізичний рівень 100Base-T4

100BaseT4 – версія, що використовує 4 витих пари категорії не нижче 3 (рис. 4.13). Окрім однонаправлених пар, використовуваних в *100BaseTX* і *10BaseT*, тут дві додаткові пари є двонаправленими і служать для розпаралелювання передачі даних. Кадр передається трьома лініями паралельно, що дозволяє понизити пропускну здатність кожної пари до 33,3 Мбіт/с. Четверта пара при передачі використовується для прослуховування сигналу від протилежного передавача – за його появою визначається факт колізії.

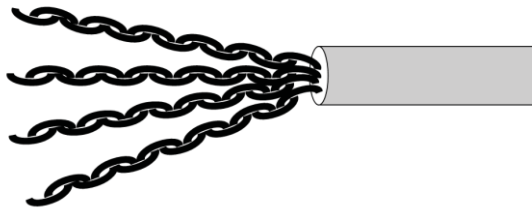


Рис. 4.13. Кабель 4 витих пар категорії 3 і вище

Центральним пристроєм в Fast Ethernet може бути комутатор. Сучасні комутатори Fast Ethernet підтримують як протокол Fast Ethernet, так і Ethernet для поєднання старих мережевих елементів, які ще використовуються на практиці і нових мереж з великою пропусною здатністю. Подібний комутатор має назву Switch 10/100 Mb/s. Комутатори 3 та 4 рівня мають окремий порт для з'єднання між комутаторами та від 8 портів та більше для підключення робочих станцій.

Однією з важливих характеристик мережі є її розмір. Це розмір зони конфлікту (області колізії, collision domain). При цьому треба враховувати, що включення в мережу одного комутатора дозволяє збільшити повний розмір мережі удвічі, що вплинуло на побудову сучасних мереж тільки на базі комутаторів.

Вибір конфігурації Ethernet

При виборі конфігурації мережі Ethernet, що складається з сегментів різних типів, виникає багато питань, пов'язаних, перш за все з максимально

допустимим розміром (діаметром) мережі і максимально можливим числом різних елементів [9; 26; 43]. Відповідно до методу CSMA/CD мережа Ethernet буде працездатною тільки в тому випадку, якщо максимальна затримка розповсюдження сигналу в ній не перевищить граничної величини.

Для отримання складних конфігурацій Ethernet з окремих сегментів раніше використовувались концентратори двох основних типів:

- репітерні концентратори, які є набором репітерів і ніяк логічно не розділяють сегменти, підключені до них;
- комутуючі (switching) концентратори або комутатори, які передають інформацію між сегментами, але не передають конфлікти з сегменту на сегмент.

У разі складніших комутуючих концентраторів конфлікти в окремих сегментах розв'язуються на місці, в самих сегментах, і не розповсюджуються по мережі, як у разі простіших репітерних концентраторів. Це має принципове значення для вибору топології мережі Ethernet, оскільки використовуваний в ній метод доступу CSMA/CD припускає наявність конфліктів і їх вирішення, причому загальна довжина мережі якраз і визначається розміром зони конфлікту, області колізії (collision domain). Таким чином, застосування репітерного концентратора не розділяє зону конфлікту, тоді як кожен комутуючий концентратор (комутатор) ділить зону конфлікту на частини. У разі комутатора оцінювати працездатність треба для кожної частини мережі *окремо*, а у разі репітерних концентраторів треба оцінювати працездатність всієї мережі *в цілому*.

Допустимі розміри мережі Ethernet визначаються наступними вимогами.

1. Обмеження на довжину кабельного сегменту, пов'язані із згасанням і спотворенням форми сигналу. Для типових інтерфейсів Ethernet вони складають:

- 10Base5 – 500 м і правило „5 – 4 – 3”;
- 10Base2 – 185 (300) м і правило „5 – 4 – 3”;
- 10BaseT/100BaseTX/100BaseT4 – 100 м.

2. Обмеження на кількість вузлів в домені колізій: не більш 1024.

3. Обмеження на кількість повторювачів між будь-якою парою вузлів: Ethernet– 4, Fast Ethernet– 1 або 2, Gigabit Ethernet– 1.

4. Обмеження на розмір домену колізій, пов'язані з часом розповсюдження сигналу між кінцевими вузлами мережі: час подвійного

обороту для Ethernet і Fast Ethernet не повинен перевищувати 512 bt, для Gigabit Ethernet – 2048 bt.

Максимальна конфігурація мережі Ethernet.

При виборі конфігурації мережі Ethernet, що складається з сегментів різних типів, виникає багато питань, зв'язаних, перш за все з максимально допустимим розміром (діаметром) мережі і максимально можливою кількістю різних елементів. Відповідно до методу CSMA/CD мережа Ethernet буде працездатною тільки в тому випадку, якщо максимальна затримка розповсюдження сигналу в ній не перевищить граничної величини.

Для отримання складних конфігурацій Ethernet з окремих сегментів застосовуються концентратори або комутатори. У разі складніших комутуючих концентраторів конфлікти в окремих сегментах розв'язуються на місці, в самих сегментах, і не розповсюджуються по мережі, як у разі простіших репітерних концентраторів.

Це має принципове значення для вибору топології мережі Ethernet, оскільки використовуваний в ній метод доступу CSMA/CD припускає наявність конфліктів і їх вирішення, причому загальна довжина мережі якраз і визначається розміром зони конфлікту, області колізії (collision domain). Таким чином, застосування репітерного концентратора не розділяє зону конфлікту, тоді як кожен комутуючий концентратор ділить зону конфлікту на частини. У разі комутатора оцінювати працездатність треба для кожної частини мережі *окремо*, а у разі репітерних концентраторів треба оцінювати працездатність всієї мережі *в цілому*.

Розвиток технології Ethernet рухається по шляху все більшого відходу від первісного стандарту. Застосування нових середовищ передачі і комутаторів дозволяє істотно збільшити розмір мережі. Відмова від манчестерського коду (в мережі Fast Ethernet і Gigabit Ethernet) забезпечує збільшення швидкості передачі даних і зниження вимог до кабелю. Відмова від методу керування CSMA/CD (при повнодуплексному режимі обміну) дає можливість різко підвищити ефективність роботи й зняти обмеження з довжини мережі. Проте, всі нові різновиди мережі також називаються мережею Ethernet.

Домен колізій

В технології Ethernet, незалежно від застосовуваного стандарту фізичного рівня, існує поняття домену колізій.

Домен колізій (collision domain) – це частина мережі Ethernet, всі вузли якої розпізнають колізію незалежно від того, у якій частині цієї мережі колізія виникла. Мережа Ethernet, побудована на повторювачах, завжди утворює один

домен колізій. Домен колізій відповідає одному поділюваному середовищу. Мости, комутатори і маршрутизатори ділять мережу Ethernet на декілька доменів колізій.

Наведена на рис. 4.14 мережа являє собою один домен колізій. Якщо, наприклад, зіткнення кадрів відбулося в концентраторі 4, то відповідно до логіки роботи концентраторів 10 Base-T сигнал колізії пошириться за всіма портами всіх концентраторів.

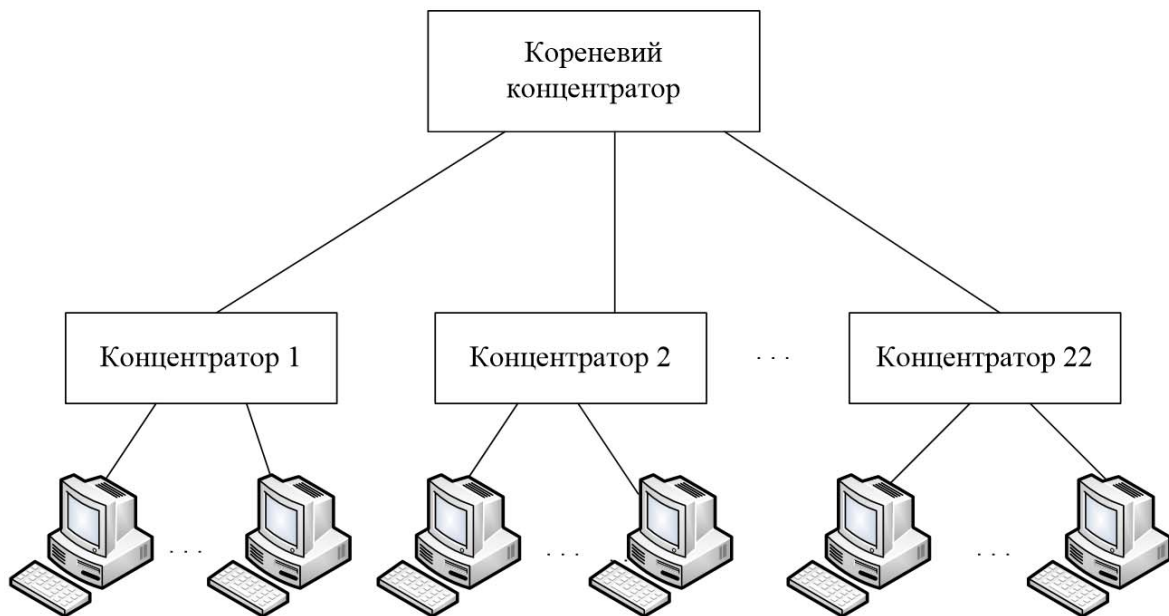


Рис. 4.14. Ієрархічне з'єднання концентраторів Ethernet

Вузли, що утворюють один домен колізій, працюють синхронно, як єдина розподілена електронна схема.

4.2. Технологія Token Ring (802.5)

Мережа *Token-Ring* (маркерне кільце) була запропонована компанією IBM в 1985 році (перший варіант з'явився в 1980 році). Вона призначалася для об'єднання в мережу всіх типів комп'ютерів, що випускаються IBM. Уже той факт, що її підтримує компанія IBM, найбільший виробник комп'ютерної техніки, говорить про те, що їй необхідно приділити особливу увагу. Але не менш важливо і те, що Token-Ring є в наш час міжнародним стандартом IEEE 802.5 (хоча між Token-Ring і IEEE 802.5 є незначні відмінності). Це ставить дану мережу на один рівень за статусом з Ethernet. Розроблялася Token-Ring як надійна альтернатива Ethernet. І хоча зараз Ethernet витісняє всі інші

мережі, Token-Ring не можна вважати безнадійно застарілою. Більш 10 мільйонів комп'ютерів у світі об'єднані цією мережею. Компанія IBM зробила все для максимально широкого поширення своєї мережі: була випущена докладна документація аж до принципових схем адаптерів. В результаті багато компаній, наприклад, 3COM, Novell, Western Digital, Proteon і інші приступилися до виробництва адаптерів. До речі, спеціально для цієї мережі, а також для іншої мережі IBM PC Network була розроблена концепція NetBIOS. Якщо в створеній раніше мережі PC Network програми NetBIOS зберігалися в убудованій в адаптер постійної пам'яті, то в мережі Token-Ring уже застосовувалася емулююча NetBIOS програма. Це дозволило більш гнучко реагувати на особливості апаратури й підтримувати сумісність із програмами більш високого рівня.

Мережа Token-Ring має топологію кільце, хоча зовні вона більше нагадує зірку. Це пов'язане з тим, що окремі абоненти (комп'ютери) приєднуються до мережі не прямо, а через спеціальні концентратори або багатостанційні пристрої доступу (MSAU або MAU – Multistation Access Unit). Фізично мережа утворює зірково-кільцеву топологію (рис. 4.15). У дійсності ж абоненти поєднуються все-таки в кільце, тобто кожний з них передає інформацію одному сусідньому абоненту, а приймає інформацію від іншого.

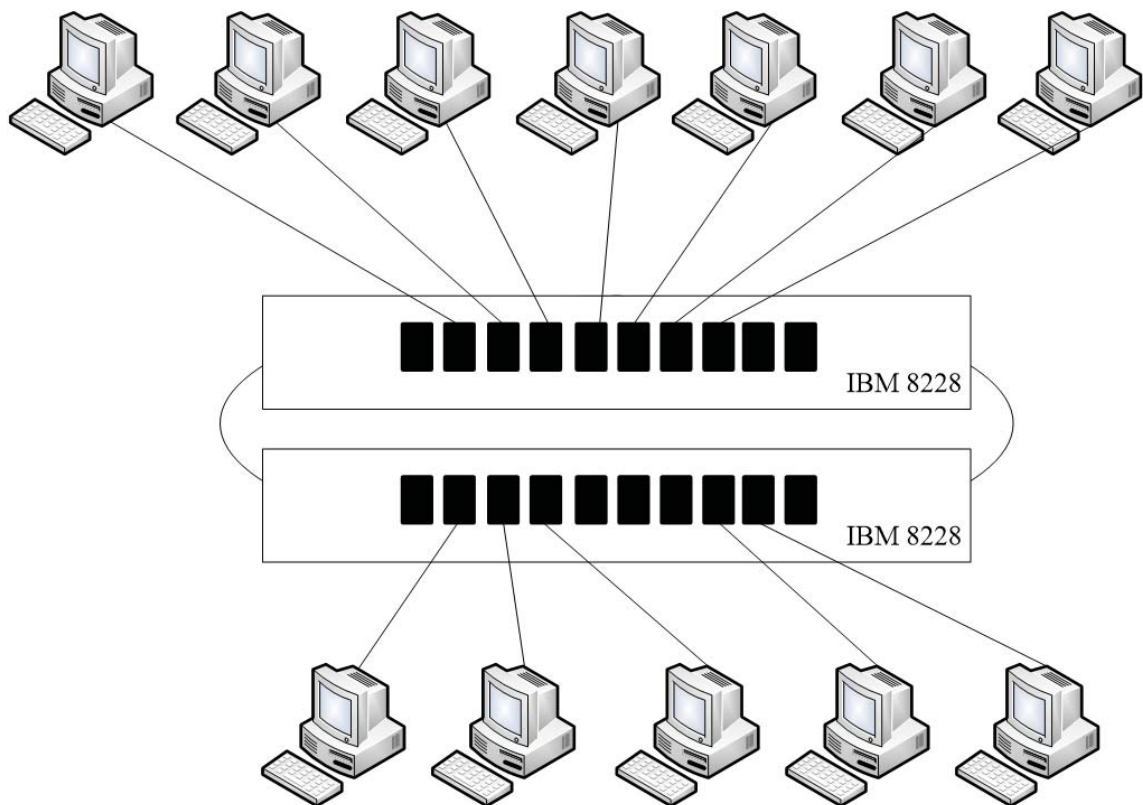


Рис. 4.15. Топологія Token Ring (фізична зірка/логічне кільце).

Концентратор (MAU) при цьому дозволяє централізувати завдання конфігурації, відключення несправних абонентів, контроль роботи мережі і т.д. (рис. 4.16). Ніякої обробки інформації він не здійснює.

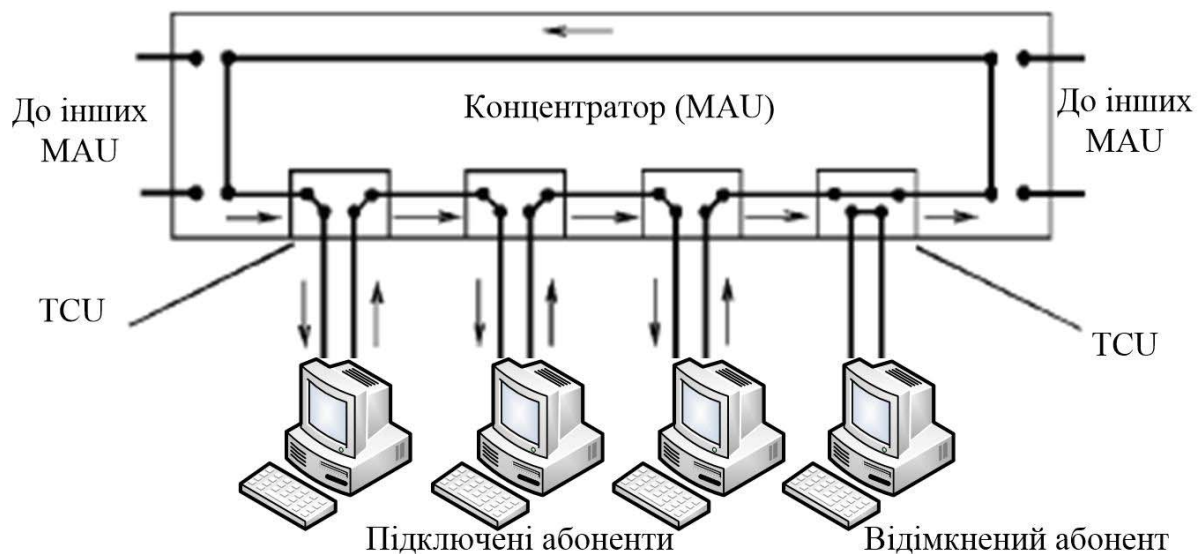


Рис. 4.16. З'єднання абонентів мережі Token-Ring у кільце за допомогою концентратора (MAU)

Для кожного абонента в складі концентратора застосовується спеціальний блок підключення до магістралі (TCU – Trunk Coupling Unit), що забезпечує автоматичне включення абонента в кільце, якщо він підключений до концентратора й справний. Якщо абонент відключається від концентратора або ж він несправний, то блок TCU автоматично відновлює цілісність кільця без участі даного абонента. Спрацьовує TCU за сигналом постійного струму (так званий “фантомний” струм), що приходить від абонента, що бажає ввімкнутися в кільце. Абонент може також відключитися від кільця й провести процедуру самотестування (крайній правий абонент на рис. 4.16). “Фантомний” струм ніяк не впливає на інформаційний сигнал, тому що сигнал у кільці не має постійної складової.

Окремі абоненти (комп'ютери) приєднуються до мережі через спеціальні концентратори MAU – (*Multistation Access Unit*).

Існують як пасивні, так і активні концентратори MAU. Активний концентратор відновлює сигнал, що приходить від абонента (тобто працює, як концентратор Ethernet). Пасивний концентратор не виконує відновлення сигналу, тільки перекомутує лінії зв'язку.

Концентратор в мережі може бути єдиним (як на рис. 4.16), у цьому випадку в кільце замикаються тільки абоненти, підключені до нього. Зовні така топологія виглядає, як зірка. Якщо ж потрібно підключити до мережі більше восьми абонентів, то декілька концентраторів з'єднуються магістральними кабелями та утворюють зірковокільцеву топологію.

Як *середовище передачі* в мережі IBM Token-Ring спочатку застосовувалася вита пара, як неекранована (UTP), так і екранована (STP), але потім з'явилися варіанти апаратури для коаксіального кабелю, а також для оптоволоконого кабелю в стандарті FDDI. Основні технічні характеристики класичного варіанта мережі Token-Ring:

- максимальна кількість концентраторів типу IBM 8228 MAU – 12;
- максимальна кількість абонентів в мережі – 96;
- максимальна довжина кабелю між абонентом і концентратором – 45 м;
- максимальна довжина кабелю між концентраторами – 45 м;
- максимальна довжина кабелю, що з'єднує всі концентратори – 120 м;
- швидкість передачі даних – 4 Мбіт/с і 16 Мбіт/с.

Всі наведені характеристики відносяться до випадку використання неекранованої витної пари. Якщо застосовується інше *середовище передачі*, характеристики мережі можуть відрізнятися. Наприклад, при використанні екранованої витної пари (STP) кількість абонентів може бути збільшена до 260 (замість 96), довжина кабелю – до 100 м (замість 45), кількість концентраторів – до 33, а повна довжина кільця, що з'єднує концентратори – до 200 м.

Оптоволоконний кабель дозволяє збільшувати довжину кабелю до двох кілометрів.

Для передачі інформації в Token Ring застосовується біфазний код (точніше, його варіант із обов'язковим переходом у центрі бітового інтервалу). Як і в будь-якій зіркоподібній топології, ніяких додаткових заходів по електричному узгодженню та зовнішньому заземленню не потрібно. Узгодження виконується апаратурою мережних адаптерів і концентраторів.

Для приєднання кабелів в Token Ring використовуються з'єднувачі RJ-45 (для неекранованої витної пари), а також MIC і DB9P. Для з'єднання однойменних контактів використовуються так звані “прямі” кабелі.

Мережа Token Ring у класичному варіанті уступає мережі Ethernet як за припустимим розміром, так і за максимальною кількістю абонентів. Що стосується швидкості передачі, то на даний час є версії Token Ring на швидкість 100 Мбіт/с (High Speed Token Ring, HSTR) і на 1000 Мбіт/с (Gigabit Token Ring). Компанії, що підтримують Token Ring (серед яких IBM, Olicom, Madge), не мають наміру відмовлятися від своєї мережі, розглядаючи її як гідного конкурента Ethernet.

У порівнянні з апаратурою Ethernet апаратура Token Ring помітно дорожча, тому що використовується більш складний *метод керування* обміном, тому мережа Token Ring не одержала настільки широкого поширення.

Однак на відміну від Ethernet мережа Token Ring значно краще тримає високий рівень навантаження (більш 30 – 40%) і забезпечує гарантований час доступу. Це необхідно, наприклад, в мережах виробничого призначення, у яких затримка реакції на зовнішню подію може привести до серйозних аварій.

В мережі Token Ring використовується класичний маркерний метод доступу, тобто по кільцю постійно циркулює маркер, до якого абоненти можуть приєднувати свої пакети даних. Звідси треба таке важливе достоїнство даної мережі, як відсутність конфліктів, але є й недоліки, зокрема необхідність контролю цілісності маркера і залежність функціонування мережі від кожного абонента (у випадку несправності абонент обов'язково повинен бути виключений з кільця).

Кожний абонент мережі (його мережний адаптер) повинен виконувати наступні функції:

- виявлення помилок передачі;
- контроль конфігурації мережі (відновлення мережі при виході з ладу того абонента, що передує йому в кільці);
- контроль численних часових співвідношень, прийнятих у мережі.

Велика кількість функцій, звичайно, ускладнює й здорожує апаратуру мережного адаптера.

Для контролю цілісності маркера в мережі використовується один з абонентів (так званий активний монітор). При цьому його апаратура нічим не відрізняється від інших, але його програмні засоби стежать за часовими співвідношеннями в мережі й формують якщо буде потреба новий маркер.

Активний монітор виконує наступні функції:

- запускає в кільце маркер на початку роботи й при його зникненні;
- регулярно (раз в 7 с) повідомляє про свою присутність спеціальним керуючим пакетом (AMP – Active Monitor Present);
- видаляє з кільця пакет, що не був вилучений його абонентом, що послав;
- стежить за припустимим часом передачі пакета.

Активний монітор вибирається при ініціалізації мережі, їм може бути будь-який комп'ютер мережі, але, як правило, стає перший включений у мережу абонент. Абонент, що став активним монітором, включає в мережу свій буфер, що гарантує, що маркер буде вміщатися в кільці навіть при мінімальній довжині кільця. Розмір цього буфера – 24 біта для швидкості 4 Мбіт/с і 32 біта для швидкості 16 Мбіт/с.

Кожний абонент постійно стежить за тим, як активний монітор виконує свої обов'язки. Якщо активний монітор з якоїсь причини виходить із ладу, то включається спеціальний механізм, за допомогою якого всі інші абоненти (запасні, резервні монітори) ухвалюють рішення щодо призначення нового активного монітора. Для цього абонент, що виявив аварію активного монітора, передає по кільцю керуючий пакет (пакет запиту маркера) зі своїм MAC-адресом. Кожний наступний абонент порівнює MAC-адресу з пакета із власним. Якщо його власна адреса менше, вона передає пакет далі без змін. Якщо ж більше, то він встановлює в пакеті свою MAC-адресу. Активним монітором стане той абонент, у якого значення MAC-адреси більш, ніж в інших (він повинен тричі одержати назад пакет зі своєю MAC-адресою). Ознакою виходу з ладу активного монітора є невиконання ним однієї з перерахованих функцій [9].

4.2.1. Маркерний метод доступу до середовища

В мережах з *маркерним методом* доступу право на доступ до середовища передається циклічно від комп'ютера до комп'ютера по логічному кільцю за допомогою спеціального кадру – *маркера* (токена) (як ви пам'ятаєте, доступ до середовища передачі в Ethernet відбувається за випадковим алгоритмом). В мережі Token Ring кільце утворюється відрізками кабелю, що з'єднують сусідні станції. Таким чином, кожна станція пов'язана з своєю передуючою і подальшою станцією і може безпосередньо обмінюватися даними тільки з ними. Для забезпечення доступу станцій до фізичного середовища кільцем циркулює кадр спеціального формату і

призначення – маркер. В мережі Token Ring будь-яка станція завжди безпосередньо одержує дані тільки від станції, яка є попередньою в кільці. Передає дані комп'ютер завжди тільки подальшому сусідньому комп'ютеру.

Одержавши маркер, станція аналізує його і за відсутності у неї даних для передачі забезпечує його просування до наступної станції. Станція, яка має дані для передачі, при отриманні маркера вилучає його з кільця, що дає їй право доступу до фізичного середовища і передачі своїх даних. Потім ця станція видає в кільце кадр даних.

Час володіння середовищем, що розділяється, в мережі Token Ring обмежується *часом утримання маркера (token holding time)*, після закінчення якого станція зобов'язана припинити передачу власних даних (поточний кадр дозволяється завершити) і передати маркер далі по кільцю. Станція може встигнути передати за час утримання маркера один або декілька кадрів залежно від розміру кадрів і величини часу утримання маркера. Зазвичай час утримання маркера за замовчанням дорівнює 10 мс. Максимальний розмір кадру для мереж 4 Мбіт/с звичайне рівний 4 Кбайт, а для мереж 16 Мбіт/с – 16 Кбайт. Такі розміри вибрані з розрахунком, що за час утримання маркера станція повинна встигнути передати хоча би один кадр. Таким чином, при швидкості 4 Мбіт/с за час 10 мс можна передати не 4 Кб, а 5 Кб, тобто максимальні розміри кадру вибрані з деяким запасом.

Передані дані проходять кільцем завжди в одному напрямку від однієї станції до іншої. Всі станції кільця ретранслюють кадр побітно, як повторювачі. Кадр забезпечений адресою призначення і адресою джерела. Якщо кадр проходить через станцію призначення, то, розпізнавши свою адресу, ця станція копіює кадр в свій внутрішній буфер і вставляє в кадр ознаку підтвердження прийому. Станція, що видала кадр даних в кільце, при зворотному його отриманні з підтвердженням прийому вилучає цей кадр з кільця і передає в мережу новий маркер для забезпечення можливості іншим станціям мережі передавати дані.

Для різних видів повідомлень, передаваним кадрам, можуть призначатися різні *пріоритети*: від 0 (нижчий) до 7 (вищий). Рішення про пріоритет конкретного кадру ухвалює станція, що передає. Маркер також завжди має деякий рівень поточного пріоритету. Станція має право захопити переданий їй маркер тільки в тому випадку, якщо пріоритет кадру, який вона хоче передати, вище (або рівний) пріоритету маркера. Інакше станція зобов'язана передати маркер до наступної по кільцю станції. За наявності в мережі маркера, причому єдиної його копії, відповідає активний монітор.

Якщо активний монітор не одержує маркер протягом тривалого часу (наприклад, 2,6 с), то він породжує новий маркер.

Технологія Token Ring дозволяє використовувати для з'єднання кінцевих станцій і концентраторів наступні типи кабелю: неекранована вита пара категорії 3 (UTP Type 3), неекранована вита пара категорії 5 (UTP Type 5), екранована вита пара (STP Type 1), а також волоконно-оптичний кабель.

4.2.2. Формати кадрів технології Token Ring (802.1)

Маркер мережі Token-Ring являє собою керуючий пакет, що містить усього три байти (рис. 4.17): байт початкового роздільника (SD – Start Delimiter), байт керування доступом (AC – Access Control) і байт кінцевого роздільника (ED – End Delimiter). Всі ці три байти входять також до складу інформаційного пакета, що правда, функції їх у маркері та у пакеті декілька розрізняються.

Початковий і кінцевий роздільники являють собою не просто послідовність нулів і одиниць, а містять сигнали спеціального виду. Це було зроблено для того, щоб роздільники не можна було поплутати ні з якими іншими байтами пакетів.

Початковий розділювач (1 байт)	Управління доступом (1 байт)	Кінцевий розділювач (1 байт)

Рис. 4.17. Формат маркера мережі Token-Ring

Початковий роздільник SD містить чотири нестандартних бітових інтервали (рис. 4.18). Два з них, що позначаються J, являють собою низький рівень сигналу протягом усього бітового інтервалу. Два інших біти, що позначаються K, являють собою високий рівень сигналу протягом усього бітового інтервалу. Зрозуміло, що такі збої в синхронізації легко виявляються приймачем. Біти J і K ніколи не можуть зустрічатися серед бітів корисної інформації.

SD							ED						
j	k	0	j	k	0	0	0	j	k	1	j	k	1
													1
													E

Рис. 4.18. Формати початкового (SD) і кінцевого (ED) роздільників

Кінцевий роздільник ED також містить у собі чотири біти спеціального виду (два біти J і два біти K), а також два одиничних біти. Але, крім того, до нього входять і два інформаційних біти, які мають сенс тільки в складі інформаційного пакета:

Бит I (Intermediate) являє собою ознаку проміжного пакета (1 відповідає першому в ланцюжку або проміжному пакету, 0 – останньому в ланцюжку або єдиному пакету).

Бит E (Error) є ознакою виявленої помилки (0 відповідає відсутності помилок, 1 – їх наявності).

Байт керування доступом (AC – Access Control) розділений на чотири поля (рис. 4.19): поле пріоритету (три біти), біт маркера, біт монітора й поле резервування (три біти).

AC

P	P	P	T	M	R	R	R

P – біти пріоритету, T – біт маркеру, M – біт монітору,
R – біти резервування

Рис. 4.19. Формат байта керування доступом

Біти (поле) пріоритету дозволяють абоненту привласнювати пріоритет своїм пакетам або маркеру (пріоритет може бути від 0 до 7, причому 7 відповідає найвищому пріоритету, а 0 – нижчому). Абонент може приєднати до маркера свій пакет тільки тоді, коли його власний пріоритет (пріоритет його пакетів) такий же або вище пріоритету маркера.

Біт маркера визначає, приєднаний чи ні пакет до маркера (одиниця відповідає маркеру без пакета, нуль – маркеру з пакетом). Біт монітора, встановлений в одиницю, говорить про те, що даний маркер переданий активним монітором.

Біти (поле) резервування дозволяють абоненту зарезервувати своє право на подальше захоплення мережі, тобто зайняти чергу на обслуговування. Якщо пріоритет абонента (пріоритет його пакетів) вище, ніж поточне значення поля резервування, то він може записати туди свій пріоритет замість колишнього. Після обходу по кільцю в полі резервування буде записаний найвищий пріоритет із всіх абонентів. Зміст поля резервування аналогічно вмісту поля пріоритету, але говорить про майбутній пріоритет.

В результаті використання полів пріоритету та резервування забезпечується можливість доступу до мережі тільки абонентам, що мають пакети для передачі з найвищим пріоритетом. Менш пріоритетні пакети будуть обслуговуватися тільки по вичерпанні більш пріоритетних пакетів.

Формат інформаційного пакета (кадру) Token Ring наведений на рис. 4.20. Крім початкового та кінцевого роздільників, а також байта керування доступом у цей пакет входять також байт керування пакетом, мережні адреси приймача та передавача, дані, контрольна сума й байт стану пакета.

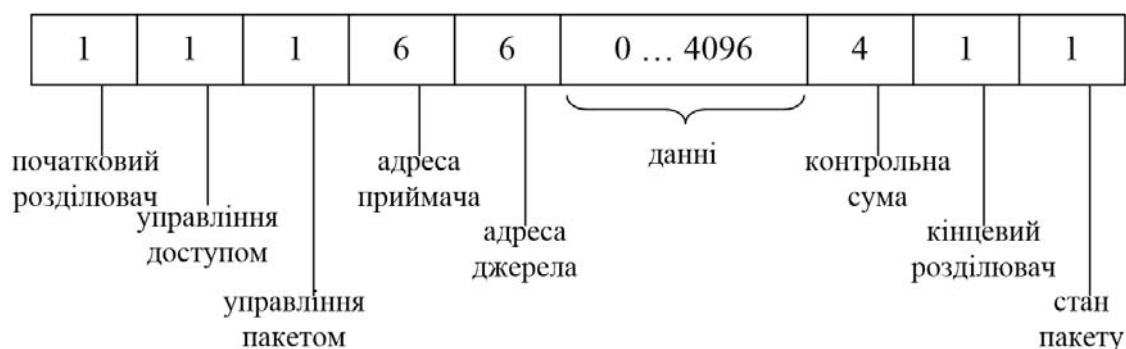


Рис. 4.20. Формат пакета (кадру) мережі Token Ring
(довжина полів дана в байтах)

Призначення полів кадру.

Початковий роздільник (SD) є ознакою початку кадру, формат – такий же, як і в маркері.

Байт управління доступом (AC) має той же формат, що й у маркері.

Байт управління пакетом (FC – Frame Control) визначає тип кадру.

Шестибайтові MAC-адреси відправника і одержувача кадру мають стандартний формат.

Поле даних (Data) містить у собі передані дані (в інформаційному пакеті) або інформацію для управління обміном (у керуючому кадрі).

Поле контрольної суми (FCS – Frame Check Sequence) являє собою 32-розрядну циклічну контрольну суму кадру (CRC).

Кінцевий роздільник (ED), як і в маркері, указує на кінець кадру. Крім того, він визначає, чи є даний кадр проміжним або заключним у послідовності переданих кадрів, а також містить ознаку помилковості кадру (рис. 4.20).

Байт стану кадру (FS – Frame Status) говорить про те, що відбувалося з даним кадром: чи був він побачений приймачем (тобто, чи існує приймач із

заданою адресою) і скопійований в пам'ять приймача. Відправник кадру довідається, чи дійшов кадр за призначенням і без помилок або його треба передавати заново.

Слід зазначити, що великий припустимий розмір переданих даних в одному кадрі в порівнянні з мережею *Ethernet* може стати вирішальним фактором для збільшення продуктивності мережі. Теоретично для швидкостей передачі 16 Мбіт/с і 100 Мбіт/с довжина поля даних може досягати навіть 18 Кбайт, що принципово при передачі великих обсягів даних. Але навіть при швидкості 4 Мбіт/с завдяки маркерному методу доступу мережа Token Ring часто забезпечує більшу фактичну швидкість передачі, ніж мережа Ethernet (10 Мбіт/с). Особливо помітна перевага Token Ring при великих навантаженнях (понад 30 – 40%), тому що в цьому випадку метод CSMA/CD вимагає багато часу на дозвіл повторних конфліктів.

Абонент, що бажає передавати кадр, чекає приходу вільного маркера і захоплює його. Захоплений маркер перетворюється в обрамлення інформаційного кадру. Потім абонент передає інформаційний кадр у кільце та чекає його повернення. Після цього він звільняє маркер і знову посилає його в мережу.

Крім маркера й звичайного кадру в мережі Token Ring може передаватися спеціальний керуючий кадр, що служить для переривання передачі (Abort). Він може бути посланий у будь-який момент і в будь-якому місці потоку даних. Кадр цей складається із двох однобайтових полів – початкового (SD) і кінцевого (ED) роздільників описаного формату.

Цікаво, що в більш швидкій версії Token Ring (16 Мбіт/с і вище) застосовується так званий метод раннього формування маркера (ETR – Early Token Release). Він дозволяє уникнути непродуктивного використання мережі в той час, поки кадр даних не повернеться по кільцю до свого відправника.

В мережі Token Ring передбачене також використання мостів і комутаторів. Вони застосовуються для поділу великого кільця на декілька кільцевих сегментів, що мають можливість обміну кадрами між собою. Це дозволяє знизити навантаження на кожний сегмент і збільшити частку часу, надавану кожному абоненту. В результаті можна сформувати розподілене кільце, тобто об'єднання декількох кільцевих сегментів одним великим магістральним кільцем (рис. 4.21) або ж зірковокільцеву структуру із центральним комутатором, до якого підключені кільцеві сегменти (рис. 4.22).

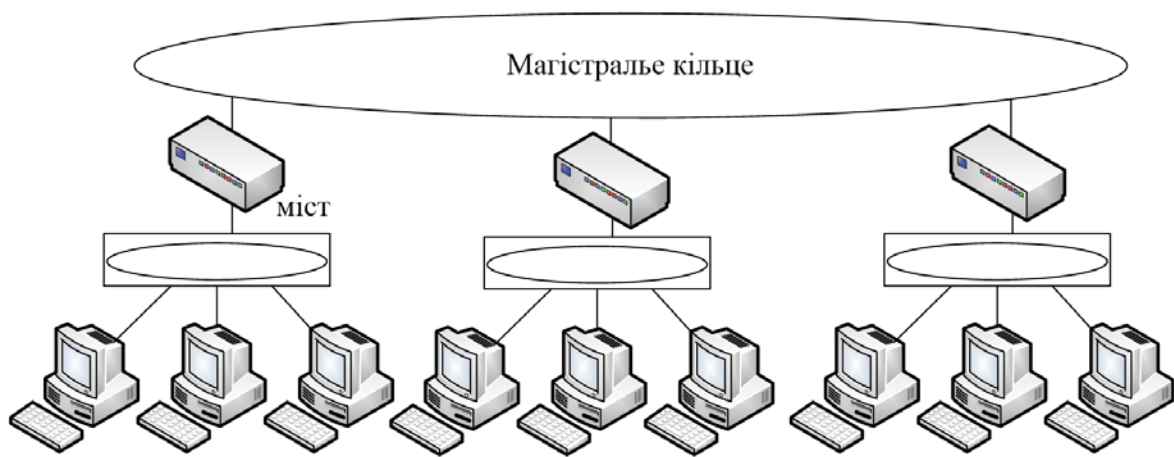


Рис. 4.21. Об'єднання сегментів магістральним кільцем за допомогою мостів

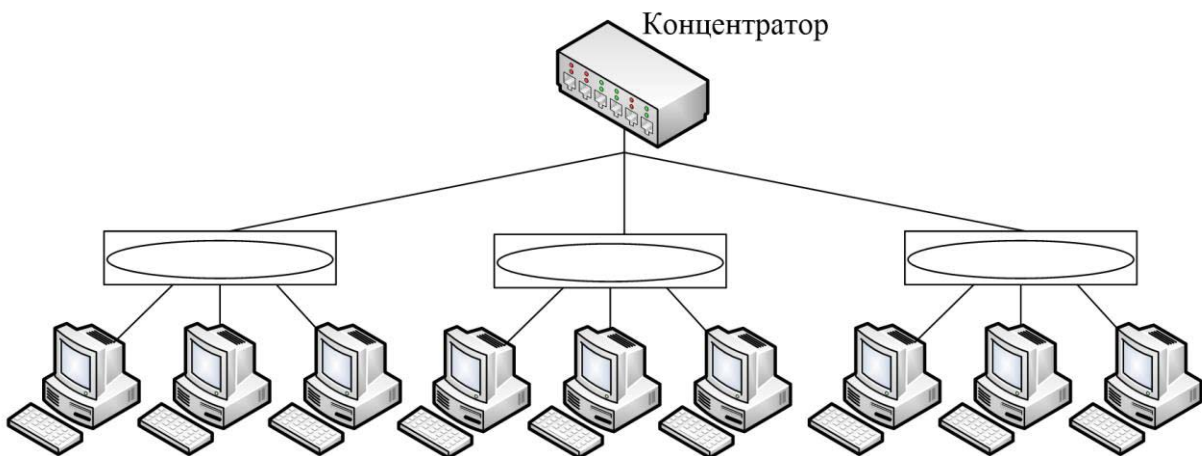


Рис. 4.22. Об'єднання сегментів центральним концентратором

4.3. Мережа Arcnet

Мережа Arcnet (або ARCnet від англійського Attached Resource Computer Net, комп'ютерна мережа з'єднаних ресурсів) – це одна з найстаріших мереж. Вона була розроблена компанією Datarpoint Corporation ще в 1977 році. Міжнародні стандарти на цю мережу відсутні, хоча саме вона вважається родоначальницею методу маркерного доступу. Незважаючи на відсутність стандартів, мережа Arcnet донедавна (в 1980 – 1990 р.р.) користувалася популярністю, навіть серйозно конкурувала з Ethernet. Велика

кількість компаній (наприклад, Datapoint, Standard Microsystems, Xircom і ін.) робили апаратуру для мережі цього типу. Але зараз виробництво апаратури Arcnet практично припинено.

Серед основних достоїнств мережі Arcnet у порівнянні з Ethernet можна назвати обмежену величину часу доступу, високу надійність зв'язку, простоту діагностики, а також порівняно низьку вартість адаптерів. До найбільш істотних недоліків мережі ставляться низька швидкість передачі інформації (2,5 Мбіт/с), система адресації й формат пакета.

Для передачі інформації в мережі Arcnet використовується код, у якому логічній одиниці відповідає два імпульси протягом бітового інтервалу, а логічному нулю – один імпульс. Очевидно, що це код, що самосинхронізується, що вимагає ще більшої пропускної здатності кабелю, ніж навіть манчестерський.

Як середовище передачі в мережі використовується коаксіальний кабель із хвильовим опором 93 Ом, приміром, марки RG-62A/U. Варіанти із витотою парою (екранованої і неекранованої) не одержали широкого поширення. Були запропоновані і варіанти на оптоволоконному кабелі, але й вони також не врятували Arcnet.

Як топологія мережа Arcnet використовує класичну шину (Arcnet-BUS), а також пасивну зірку (Arcnet-STAR). У зірці застосовуються концентратори (хаб). Можливе об'єднання за допомогою концентраторів шинних і зіркових сегментів у деревоподібну топологію (як і в Ethernet). Головне обмеження – у топології не повинне бути замкнутих шляхів (петель). Ще одне обмеження: кількість сегментів, з'єднаних послідовним ланцюжком за допомогою концентраторів, не повинне перевищувати трьох.

Основні технічні характеристики мережі Arcnet наступні.

- Середовище передачі – коаксіальний кабель, вита пара.
- Максимальна довжина мережі – 6 км.
- Максимальна довжина кабелю від абонента до пасивного концентратора – 30 м.
- Максимальна довжина кабелю від абонента до активного концентратора – 600 м.
- Максимальна довжина кабелю між активним і пасивним концентраторами – 30 м.
- Максимальна довжина кабелю між активними концентраторами – 600 м.

- Максимальна кількість абонентів в мережі – 255.
- Максимальна кількість абонентів на шинному сегменті – 8.
- Мінімальна відстань між абонентами в шині – 1 м.
- Максимальна довжина шинного сегмента – 300 м.
- Швидкість передачі даних – 2,5 Мбіт/с.

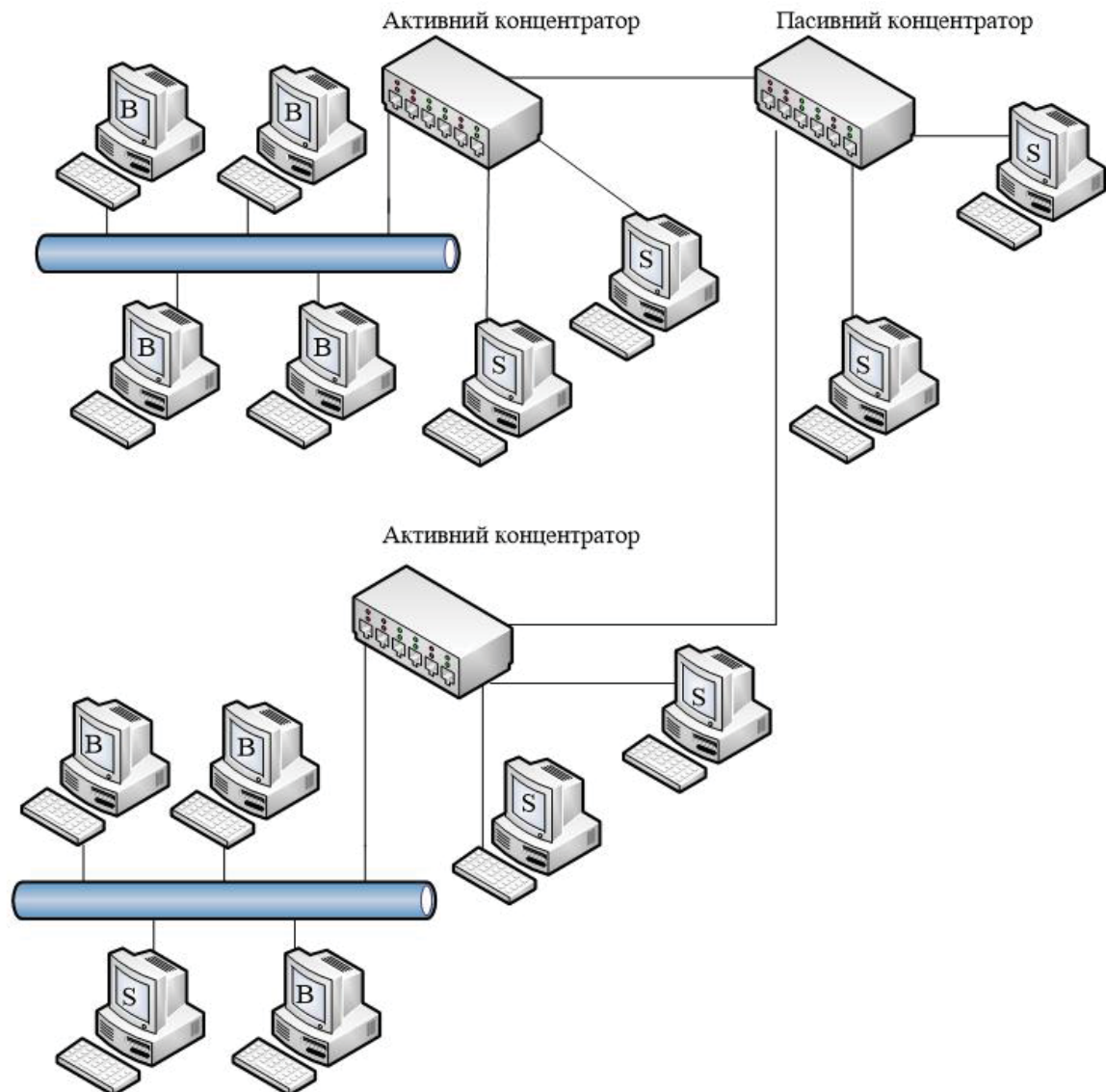


Рис. 4.23. Топологія мережі Arcnet типу шина
(В – адаптери для роботи в шині, S – адаптери для роботи в зірці)

При створенні складних топологій необхідно стежити за тим, щоб затримка поширення сигналів в мережі між абонентами не перевищувала 30 мкс. Максимальне загасання сигналу в кабелі на частоті 5 МГц не повинне перевищувати 11 дБ.

В мережі Arcnet використовується маркерний метод доступу (метод передачі права), але він трохи відрізняється від аналогічного в мережі Token-Ring. Близьче всього цей метод до того, що передбачений у стандарті IEEE 802.4.

Так само, як і у випадку Token Ring, конфлікти в Arcnet повністю виключені. Як і будь-яка маркерна мережа, Arcnet добре тримає навантаження й гарантує величину часу доступу до мережі (на відміну від Ethernet). Повний час обходу маркером всіх абонентів становить 840 мс. Відповідно, цей же інтервал визначає верхня межа часу доступу до мережі.

Маркер формується спеціальним абонентом – контролером мережі. Їм є абонент із мінімальною (нульовою) адресою.

Якщо абонент не одержує вільний маркер протягом 840 мс, то він посилає в мережу довгу бітову послідовність (для гарантованого знищення зіпсованого старого маркера). Після цього виробляється процедура контролю мережі й призначення (при необхідності) нового контролера.

Розмір пакета мережі Arcnet становить 0,5 Кбайт. Крім поля даних у нього входять також 8-бітні адреси приймача й передавача та 16-бітна циклічна контрольна сума (CRC). Такий невеликий розмір пакета виявляється не занадто зручним при високій інтенсивності обміну по мережі.

Адаптери мережі Arcnet відрізняються від адаптерів інших мереж тим, що в них необхідно за допомогою перемикачів або перемичок установити власну мережну адресу (усього їх може бути 255, тому що останній, 256-ой адреса застосовується в мережі для режиму широкого віщання). Контроль унікальності кожної адреси мережі повністю покладається на користувачів мережі. Підключення нових абонентів стає при цьому досить складним, тому що необхідно задавати ту адресу, що ще не використовувалась. Вибір 8-бітного формату адреси обмежує припустиму кількість абонентів в мережі – 255, що може бути недостатньо для великих компаній.

В результаті все це привело до практично повної відмови від мережі Arcnet. Існували варіанти мережі Arcnet, розраховані на швидкість передачі 20 Мбіт/с, але вони не одержали широкого поширення.

4.4. Технологія FDDI

Мережа *FDDI* (від англійського Fiber Distributed Data Interface, оптоволоконний розподілений інтерфейс даних) – це одна з новітніх розробок стандартів локальних мереж. Стандарт *FDDI* [2, 5, 6] був

запропонований Американським національним інститутом стандартів ANSI (специфікація ANSI X3T9.5). Потім був прийнятий стандарт ISO 9314, що відповідає специфікаціям ANSI. Рівень стандартизації мережі досить високий.

На відміну від інших стандартних локальних мереж, стандарт *FDDI* з самого початку орієнтувався на високу швидкість передачі (100 Мбіт/с) і на застосування найбільш перспективного оптоволоконного кабелю. Тому в цьому випадку розробники не були стиснуті рамками старих стандартів, що орієнтувалися на низькі швидкості та електричний кабель.

Вибір оптоволокна як *середовище передачі* визначив такі переваги нової мережі, як висока перешкодозахищеність, максимальна таємність передачі інформації і прекрасна гальванічна розв'язка абонентів. Висока швидкість передачі, що у випадку оптоволоконного кабелю досягається набагато простіше, дозволяє вирішувати багато завдань, недоступних менш швидкісним мережам, наприклад, передачу відео у реальному масштабі часу. Крім того, оптоволоконний кабель легко вирішує проблему передачі даних на відстань декількох кілометрів без ретрансляції, що дозволяє будувати великі за розмірами мережі, що охоплюють навіть цілі міста й мають при цьому всі переваги локальних мереж (зокрема, низький рівень помилок). Все це визначило популярність мережі *FDDI*, хоча вона поширена ще не так широко, як Ethernet і Token Ring.

За основу стандарту *FDDI* був узятий метод маркерного доступу, передбачений міжнародним стандартом IEEE 802.5 (Token Ring). Несуттєві відмінності від цього стандарту визначаються необхідністю забезпечити високу швидкість передачі інформації на великі відстані. Топологія мережі *FDDI* – це кільце, найбільш підходяща топологія для оптоволоконного кабелю. В мережі застосовується два різнонаправлених оптоволоконних кабелі, один із яких звичайно перебуває в резерві, однак таке рішення дозволяє використовувати також повнодуплексну передачу інформації (одночасно у двох напрямках) з подвоєною ефективною швидкістю в 200 Мбіт/с (при цьому кожний із двох каналів працює на швидкості 100 Мбіт/с). Застосовується й зірково-кільцева топологія з концентраторами, включеними в кільце (як в Token Ring).

Основні технічні характеристики мережі *FDDI*.

- Максимальна кількість абонентів мережі – 1000.
- Максимальна довжина кільця мережі – 20 км.

- Максимальна відстань між абонентами мережі – 2 км.
- Середовище передачі – багатомодовий оптоволоконний кабель (можливе застосування електричної виті пари).
- Метод доступу – маркерний.
- Швидкість передачі інформації – 100 Мбіт/с (200 Мбіт/с для дуплексного режиму передачі).

Стандарт *FDDI* має значні переваги в порівнянні з усіма розглянутими раніше мережами. Наприклад, мережа Fast Ethernet, що має таку ж пропускну здатність 100 Мбіт/с, не може зрівнятися з *FDDI* за припустимими розмірами мережі. До того ж маркерний метод доступу *FDDI* забезпечує на відміну від CSMA/CD гарантований час доступу й відсутність конфліктів при будь-якому рівні навантаження.

Обмеження на загальну довжину мережі в 20 км пов'язано не із загасанням сигналів у кабелі, а з необхідністю обмеження часу повного проходження сигналу по кільцю для забезпечення гранично припустимого часу доступу. А от максимальна відстань між абонентами (2 км при багатомодовому кабелі) визначається саме загасанням сигналів у кабелі (воно не повинне перевищувати 11 дБ). Передбачена також можливість застосування одномодового кабелю, і в цьому випадку відстань між абонентами може досягати 45 кілометрів, а повна довжина кільця – 200 км.

Є також реалізація *FDDI* на електричному кабелі (CDDI – Copper Distributed Data Interface або TPDDI – Twisted Pair Distributed Data Interface). При цьому використовується кабель категорії 5 з з'єднувачи RJ-45. Максимальна відстань між абонентами в цьому випадку повинна бути не більше 100 метрів. Вартість обладнання мережі на електричному кабелі в декілька разів менше. Але ця версія мережі вже не має настільки очевидних переваг перед конкурентами, як споконвічна оптоволоконна *FDDI*. Електричні версії *FDDI* стандартизовані набагато гірше оптоволоконних, тому сумісність обладнання різних виробників не гарантується.

Для передачі даних в *FDDI* застосовується вже згадуваний у першому розділі код 4B/5B (табл. 4.1), спеціально розроблений для цього стандарту. Головний принцип коду – уникнути довгих послідовностей нулів і одиниць. Код 4B/5B забезпечує швидкість передачі 100 Мбіт/с при пропускну здатності кабелю 125 мільйонів сигналів у секунду (або 125 МБод), а не 200 МБод, як у випадку манчестерського коду. При цьому кожним чотирьом бітам переданої інформації (кожному напівбайту або нібблу) ставиться у

відповідність п'ять переданих по кабелю бітів. Це дозволяє приймачу відновлювати синхронізацію даних, що приходять, один раз на чотири прийнятих біти. Таким чином, досягається компроміс між найпростішим кодом NRZ і манчестерським кодом, що самосинхронізується на кожному біті. Додатково сигнали кодуються кодом NRZI (у випадку TPDDI) і MLT-3 (у випадку FDDI).

Таблиця 4.1.

Код 4В/5В

Інформація	Код 4В/5В	Інформація	Код 4В/5В
0000	11110	1000	10010
0001	01001	1001	10011
0010	10100	1010	10110
0011	10101	1011	10111
0100	01010	1100	11010
0101	01011	1101	11011
0110	01110	1110	11100
0111	01111	1111	11101

4.4.1. Особливості метода доступу технології FDDI

Стандарт FDDI для досягнення високої гнучкості мережі передбачає включення в кільце абонентів двох типів:

- Абоненти (станції) класу А (абоненти подвійного підключення, DAS – Dual-Attachment Stations) підключаються до обох (внутрішніх і зовнішнього) кілець мережі. При цьому реалізується можливість обміну зі швидкістю до 200 Мбіт/с або резервування кабелю мережі (при ушкодженні основного кабелю використовується резервний). Апаратура цього класу застосовується в самих критичних з погляду швидкодії частинах мережі.
- Абоненти (станції) класу В (абоненти одинарного підключення, SAS – Single-Attachment Stations) підключаються тільки до одного (зовнішнього) кільця мережі. Вони більш прості й дешеві, у порівнянні з адаптерами класу А, але не мають їх можливостей. У мережу вони можуть включатись тільки через концентратор або обхідний комутатор, що відключає їх у випадку аварії.

Крім власне абонентів (комп'ютерів, терміналів і т.д.) в мережі використовуються зв'язні концентратори (Wiring Concentrators), включення

яких дозволяє зібрати в одне місце всі точки підключення з метою контролю роботи мережі, діагностики несправностей і спрощення реконфігурації. При застосуванні кабелів різних типів (наприклад, оптоволоконного кабелю й витої пари) концентратор виконує також функцію перетворення електричних сигналів в оптичні і навпаки. Концентратори також бувають подвійного підключення (DAC – Dual-Attachment Concentrator) і одинарного підключення (SAC – Single-Attachment Concentrator). Приклад конфігурації мережі *FDDI* представлений на рис. 4.24. Принцип об'єднання пристроїв мережі ілюструється на рис. 4.25.



Рис. 4.24. Приклад конфігурації мережі FDDI

Порт А визначений тільки для пристроїв подвійного підключення, його вхід підключається до первинного (зовнішнього) кільця, а вихід – до вторинного (внутрішнього) кільця.

Порт В визначений тільки для пристроїв подвійного підключення, його вхід підключається до вторинного (внутрішнього) кільця, а вихід – до первинного (зовнішнього) кільця. Порт А звичайно з'єднується з портом В, а порт В – з портом А.

Порт М (Master) визначений для концентраторів і з'єднує два концентратори між собою або концентратор з абонентом при одному кільці. Порт М як правило з'єднується з портом S.

Порт *S* (Slave) визначений тільки для пристроїв одинарного підключення (концентраторів і абонентів). Порт *S* звичайно з'єднується з портом *M*.

Крім абонентів (станцій) і концентраторів в мережі *FDDI* застосовуються обхідні комутатори (bypass switch). Обхідні комутатори включаються між абонентом і кільцем і дозволяють відключити абонента від кільця у випадку його несправності. Управляється обхідний комутатор електричним сигналом від абонента. Залежно від керуючого сигналу він або включає абонента в кільце або ж виключає його з кільця, замикаючи його на самого себе (рис. 4.25).

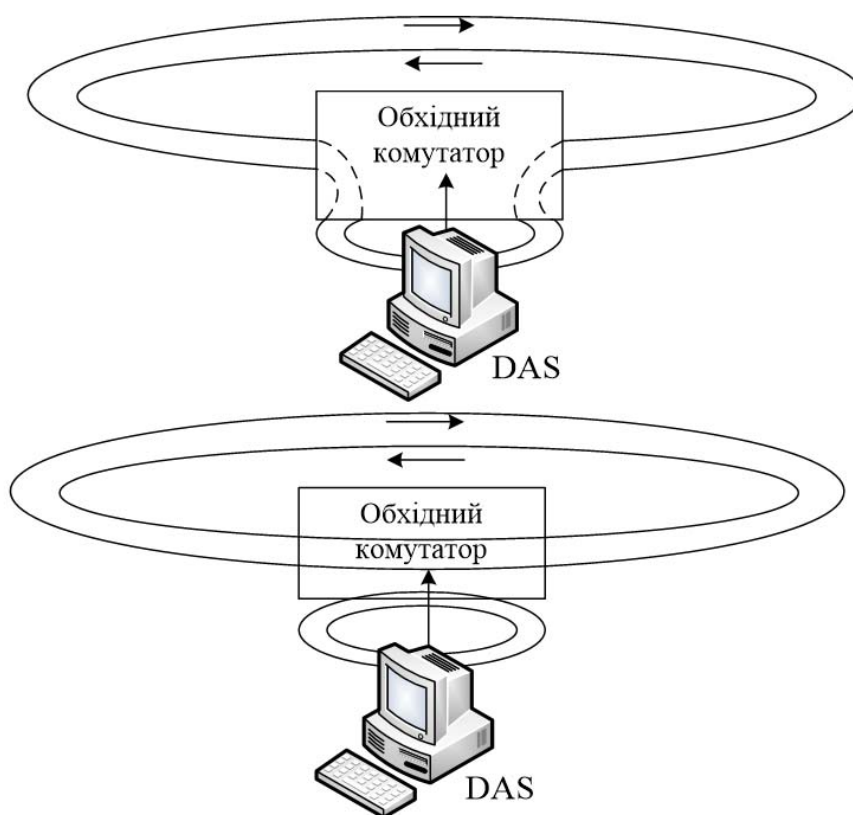


Рис. 4.25. Включення обхідного комутатора

При використанні обхідних комутаторів необхідно враховувати додаткові загасання, внесені ними (близько 2,5 дБ на один комутатор). На відміну від методу доступу, пропонованого стандартом IEEE 802.5, в *FDDI* застосовується так звана множинна передача маркера. Якщо у випадку мережі Token-Ring новий (вільний) маркер передається абонентом тільки після повернення до нього його пакета, то в *FDDI* новий маркер передається абонентом відразу ж після закінчення передачі їм пакета (подібно тому, як це робиться при методі ETR в мережі Token-Ring).

4.4.2. Порівняння з технологіями Token Ring та Ethernet

В мережі FDDI не використовується система пріоритетів і резервування, як в Token-Ring. Але передбачений механізм адаптивного планування навантаження.

Кожний абонент веде свій відлік часу, порівнюючи реальний час обігу маркера по кільцю (TRT – Token Rotation Time) із заздалегідь встановленим контрольним (операційним) часом його прибуття (T_{OPR}).

Якщо маркер вертається раніше, ніж встановлене T_{OPR}, то робиться висновок про те, що мережа завантажена мало, і, отже, абонент може передавати всю інформацію в асинхронному режимі, тобто незалежно від інших. Для цього абонент може використовувати весь часовий інтервал, що залишився (T_{OPR} - TRT).

Якщо ж маркер вертається пізніше, ніж встановлене T_{OPR}, то мережа завантажена сильно, і абонент може передавати тільки найважливішу інформацію протягом того інтервалу часу, що приділяється йому в синхронному режимі.

Величина T_{OPR} вибирається на етапі ініціалізації мережі всіма абонентами в процесі змагання.

Такий механізм дозволяє абонентам гнучко реагувати на завантаження мережі і автоматично підтримувати її на оптимальному рівні. Для правильної роботи мережі затримка проходження сигналу по кільцю повинна бути обмежена. Так, у випадку максимальної довжини кільця 200 км і максимальній кількості абонентів 1000 повний час затримки не повинен перевищувати 1,617 мс.

Формати маркера (рис. 4.26) і пакета (рис. 4.27) мережі FDDI трохи відрізняються від форматів, використовуваних в мережі Token-Ring.

Преамбула (8 байт)	Початковий роздільник (1 байт)	Управління (1 байт)	Кінцевий роздільник (1 байт)	Статус пакету (1 байт)

Рис. 4.26. Формат маркера FDDI

Призначення полів:

Преамбула (Preamble) використовується для синхронізації. Спочатку вона містить 64 біта, але абоненти, через які проходить пакет, можуть міняти її розмір.

Початковий роздільник (SD – Start Delimiter) виконує функцію ознаки початку кадру.



Рис. 4.27. Формат пакета FDDI

Байт управління (FC – Frame Control) містить інформацію про пакет (розмір поля адреси, синхронна/асинхронна передача, тип пакета – службовий або інформаційний, код команди).

Адреси приймача й джерела (SA – Source Address і DA – Destination Address) можуть бути 6-байтовими (аналогічно Ethernet і Token-Ring) або 2-байтовими.

Поле даних (Info) має змінну довжину (від 0 до 4478 байт). У службових (командних) пакетах поле даних має нульову довжину.

Поле контрольної суми (FCS – Frame Check Sequence) містить 32-бітну циклічну контрольну суму пакета (CRC).

Кінцевий роздільник (ED – End Delimiter) визначає кінець кадру.

Байт стану кадра (FS – Frame Status) містить у собі біт виявлення помилки, біт розпізнавання адреси і біт копіювання (аналогічно Token-Ring).

Формат байта управління мережі FDDI (рис. 4.28):

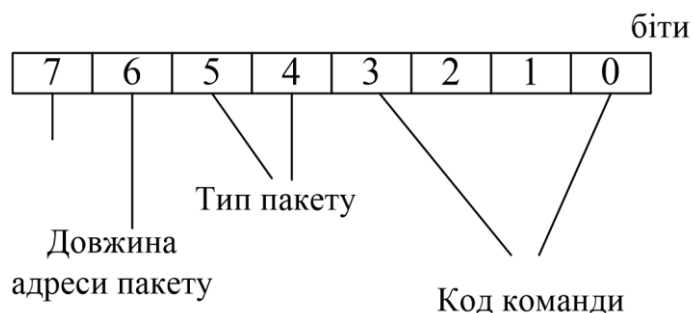


Рис. 4.28. Формат байта управління

Біт класу кадру визначає тип кадру: синхронний або асинхронний.

Біт довжини адреси встановлює, яка адреса (6-байтова або 2-байтова) використовується в даному кадрі.

Поле типу кадру (два біти) визначає, керуючий це кадр або інформаційний.

Поле коду команди (чотири біти) указує на те, яку команду повинен виконати приймач (якщо це керуючий кадр).

На закінчення необхідно відзначити, що незважаючи на очевидні переваги *FDDI* дана мережа не одержала широкого поширення, що зв'язано головним чином з високою вартістю її апаратури (порядку кількох сотень і навіть тисяч доларів). Основна область застосування *FDDI* зараз – це базові, опорні (Backbone) мережі, що поєднують декілька мереж. Застосовується *FDDI* також для з'єднання потужних робочих станцій або серверів, що вимагають високошвидкісного обміну. Передбачається, що мережа Fast Ethernet може потіснити *FDDI*, однак переваги оптоволоконного кабелю, маркерного методу управління і рекордний припустимий розмір мережі ставлять у наш час *FDDI* поза конкуренцією. А в тих випадках, коли вартість апаратури має вирішальне значення, можна на некритичних ділянках застосовувати версію *FDDI* на основі витієї пари (TPDDI). До того ж вартість апаратури *FDDI* може сильно зменшитися з ростом обсягу її випуску.

FDDI II

Спочатку стандарт *FDDI* розроблявся групою ANSI X3T9.5 (1987 – 1988 рр.), після 1995 року – ANSI X3T12. Стандарти ISO 9314-XX з'явилися декілька пізніше, вони відповідають специфікаціям ANSI. У 1993 р. з'явився стандарт *FDDI-II*, в якому визначений додатковий режим гібридного кільця для одночасної передачі ізохронного і асинхронного трафіку. Станції *FDDI-II* сумісні з *FDDI*, але спільно працювати можуть тільки в базовому режимі *FDDI*. Устаткування *FDDI-II* широкого розповсюдження не отримало. Стандарт *FDDI* визначає 4 компоненти: PMD, PHY, MAC і SMT (рис. 4.29).

Чисто електричну реалізацію архітектури *FDDI* на витій парі називають також *GDDI* (Copper Distributed Data Interface) або, же *TPDDI* (Twisted Pair Distributed Data Interface). *SDDI* має на увазі використання екранованого кабелю STP Type 1. В порівнянні з оптичним варіантом ці технології істотно дешевші, але допустима довжина ліній зв'язку між вузлами скорочується до 100 м. В порівнянні з оптичною, електричні версії менш стандартизовані і сумісність обладнання різних виробників не гарантується.

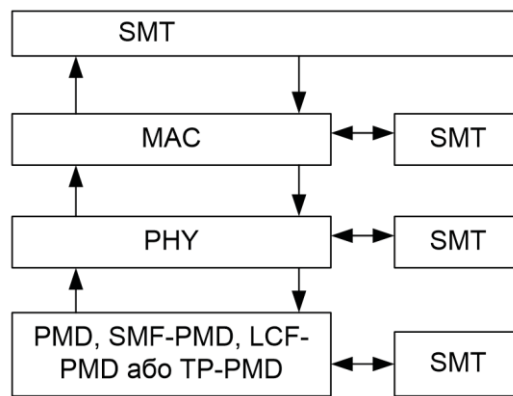


Рис. 4.29. Стандарт FDDI

В MAC-рівні FDDI-II введено два нові елементи NMUX і IMAC. Гібридний мультиплексор NMUX (Hybrid MultipleXer) має два інтерфейси Mac-підрівня, один з яких (звичайний) передає і приймає кадри LLC-підрівня, інший – ізохронний, IMAC – спілкується з одним або декількома мультиплексорами-комутаторами каналів CS-MUX (Circuit-Switched Multiplexer). За замовчанням мережа працює в базовому режимі, підтримуючи тільки комутацію пакетів. Гібридний режим включається при необхідності, він можливий, якщо всі станції кільця підтримують FDDI-II.

У гібридному режимі передача структурується у вигляді циклів-кадрів, що безперервно повторюються протягом сеансу з частотою 8000 разів в секунду. Цикли генеруються однією станцією, що є ведучою (cycle master), а решта станцій може вкладати дані в поля, що відводяться ним (і витягувати їх).

CDDI. Оптиволоконний інтерфейс FDDI, а також його розширений варіант, FDDI II спеціально адаптований для роботи з інформацією мультимедіа, і CDDI реалізовуючий FDDI на мідних кабелях. Всі версії FDDI підтримують швидкість обміну 100 Мбіт/с.

4.5. Високошвидкісна технологія Gigabit Ethernet

Швидкодія мережі Fast Ethernet і інших мереж, що працюють на швидкості в 100 Мбіт/с, у наш час задовольняє вимогам більшості завдань, але в ряді випадків навіть його виявляється недостатньо. Особливо в тих ситуаціях, коли необхідно підключати до мережі сучасні високопродуктивні сервери або будувати мережі з більшою кількістю абонентів, що вимагають високої інтенсивності обміну. Наприклад, усе більш широко застосовується мережна обробка тривимірних динамічних зображень. Швидкість комп'ютерів безупинно росте, вони забезпечують більш високі темпи обміну

із зовнішніми пристроями. В результаті мережа може виявитися найбільш слабким місцем системи, і її пропускна здатність буде основним стримуючим фактором у збільшенні швидкодії.

Роботи з досягнення швидкості передачі в 1 Гбіт/с в останні роки ведуться досить інтенсивно декількома компаніями. Однак, швидше за все, найбільш перспективною виявиться мережа *Gigabit Ethernet*. Це пов'язано, насамперед, з тим, що перехід на неї виявиться найбільш безболісним, найдешевшим і психологічно прийнятним. Адже мережа Ethernet і її версія Fast Ethernet сьогодні далеко випереджають всіх своїх конкурентів з обсягу продажів і поширеності у світі.

Мережа *Gigabit Ethernet* – це природний, еволюційний шлях розвитку концепції, закладеної в стандартній мережі Ethernet. Безумовно, вона успадковує і всі недоліки своїх прямих попередників, наприклад, негарантований час доступу до мережі. Однак величезна пропускна здатність приводить до того, що завантажити мережу до тих рівнів, коли цей фактор стає визначальним, досить важко. Зате збереження спадковості дозволяє досить просто з'єднувати сегменти Ethernet, Fast Ethernet і *Gigabit Ethernet* у мережу, і, саме головне, переходити до нових швидкостей поступово, уводячи гігабітні сегменти тільки на самих напружених ділянках мережі.

В мережі *Gigabit Ethernet* зберігається все той же, що добре зарекомендував себе в попередніх версіях, метод доступу CSMA/CD, використовуються ті ж *формати пакетів* (кадрів) і ті ж їхні розміри. Не потрібно ніякого перетворення протоколів у місцях з'єднання із сегментами Ethernet і Fast Ethernet. Єдине, що потрібно, – це узгодження швидкостей обміну, тому головною областю застосування *Gigabit Ethernet* стане в першу чергу з'єднання концентраторів Ethernet і Fast Ethernet між собою.

З появою швидкодійних серверів і поширенням персональних комп'ютерів класу “high-end” переваги *Gigabit Ethernet* стають більш явними. Так, 64-розрядна системна магістраль PCI, уже фактичний стандарт, цілком досягає необхідної для такої мережі швидкості передачі даних.

Роботи зі створення мережі *Gigabit Ethernet* ведуться з 1995 року. В 1998 році прийнятий стандарт, що одержав найменування IEEE 802.3z (1000 BASE-SX, 1000 BASE-LX і 1000 BASE-CX). Розробкою займається спеціально створений альянс (*Gigabit Ethernet Alliance*), у який, зокрема, входить така відома компанія, що займається мережною апаратурою, як 3Com. В 1999 році прийнятий стандарт IEEE 802.3ab (1000 BASE-T).

Номенклатура сегментів мережі *Gigabit Ethernet* на даний час містить у собі наступні типи:

1000 BASE-SX – сегмент на багатомодовому оптоволоконному кабелі з довжиною хвилі світлового сигналу 850 нм (довжиною до 500 м). Використовуються лазерні передавачі.

1000 BASE-LX – сегмент на багатомодовому (довжиною до 500 м) і одномодовому (довжиною до 2000 м) оптоволоконному кабелі з довжиною хвилі світлового сигналу 1300 нм. Використовуються лазерні передавачі.

1000 BASE-CX – сегмент на екранованій витій парі (довжиною до 25 м).

1000 BASE-T (стандарт IEEE 802.3ab) – сегмент на зчетвереній неекранованій витій парі категорії 5 (довжиною до 100 м). Використовується 5-рівневе кодування (PAM-5), причому в повнодуплексному режимі передача ведеться по кожній парі у двох напрямках.

Спеціально для мережі *Gigabit Ethernet* запропонований метод кодування переданої інформації 8B/10B, побудований за тим же принципом, що і код 4B/5B мережі *FDDI* (крім 1000 BASE-T). Таким чином, восьми бітам інформації, яку потрібно передати, ставиться у відповідність 10 біт, переданих по мережі. Цей код дозволяє зберегти самосинхронізацію, легко виявляти несучу (факт передачі), але не вимагає подвоєння смуги пропускання, як у випадку манчестерського коду.

Для збільшення 512-бітного інтервалів мережі Ethernet, що відповідає мінімальній довжині пакета (51,2 мкс в мережі Ethernet і 5,12 мкс в мережі Fast Ethernet) розроблені спеціальні методи. Зокрема, мінімальна довжина пакета збільшена до 512 байт (4096 біт). В протилежному випадку часовий інтервал 0,512 мкс надмірно обмежував би граничну довжину мережі *Gigabit Ethernet*. Всі пакети з довжиною менше 512 байт розширюються до 512 байт. Поле розширення вставляється в кадр після поля контрольної суми. Це вимагає додаткової обробки пакетів, але натомість максимально припустимий розмір мережі стає в 8 разів більше, ніж без прийняття таких мір.

Крім того, в *Gigabit Ethernet* передбачена можливість блокового режиму передачі кадрів (frame bursting). При цьому абонент, що одержав право передавати і, що має для передачі декілька кадрів, може передати не один, а декілька кадрів, послідовно, причому адресованих різним абонентам-одержувачам. Додаткові передані пакети можуть бути тільки короткими, а сумарна довжина всіх пакетів блоку не повинна перевищувати 8192 байта.

Таке рішення дозволяє знизити кількість захоплень мережі й зменшити число колізій. При використанні блокового режиму розширюється до 512 байт тільки перший кадр блоку для того, щоб перевірити, чи немає в мережі колізій. Інші пакети до 512 байт можуть не розширюватися.

Передача в мережі *Gigabit Ethernet* виробляється як у напівдуплексному режимі (зі збереженням методу доступу CSMA/CD), так і в більш швидкому повнодуплексному режимі (аналогічно попередньої мережі Fast Ethernet).

Мережа *Gigabit Ethernet*, насамперед, знаходить застосування в мережах, що поєднує комп'ютери великих підприємств, які розташовуються в декількох будинках. Вона дозволяє за допомогою відповідних комутаторів, що перетворюють швидкості передачі, забезпечити канали зв'язку з високою пропускною здатністю між окремими частинами складної мережі (рис. 4.30) або лінії зв'язку комутаторів зі зверхшвидкодійними серверами (рис. 4.31).

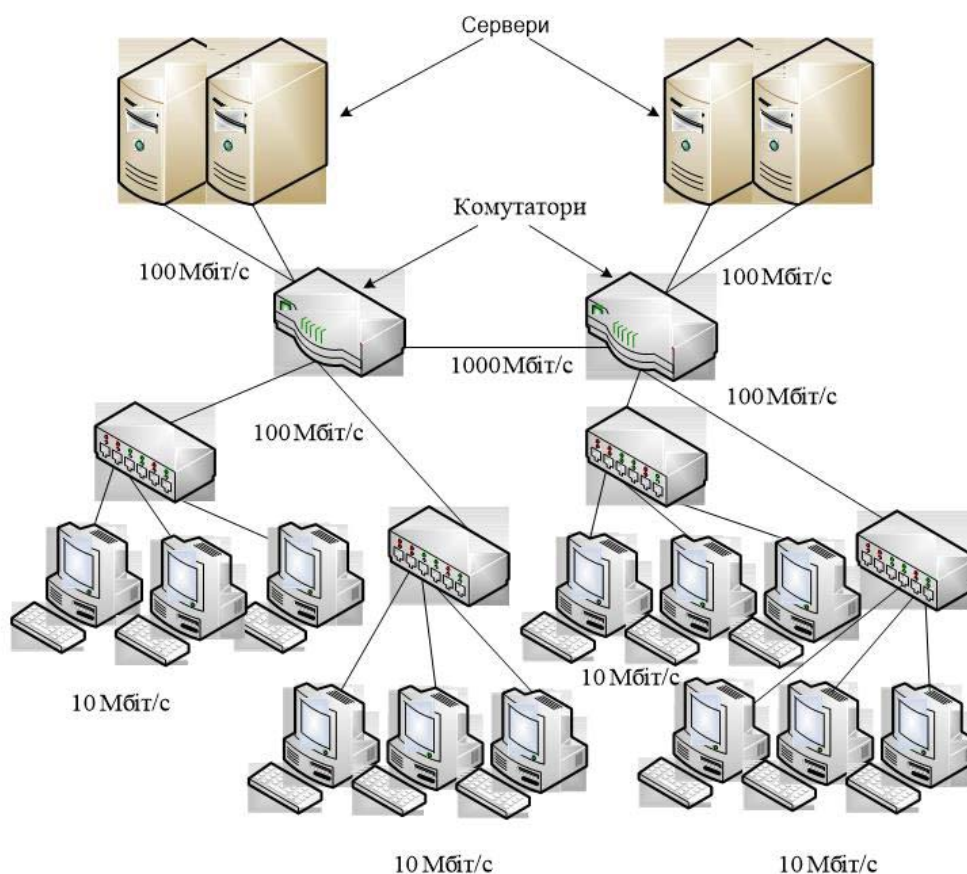


Рис. 4.30. Використання мережі Gigabit Ethernet для з'єднання груп комп'ютерів

Ймовірно, у ряді випадків *Gigabit Ethernet* буде витіснити оптоволоконну мережу *FDDI*, що у наш час все частіше використовується для об'єднання в мережу декількох локальних мереж, у тому числі, і Ethernet. Щоправда, *FDDI* може зв'язувати абонентів, що перебувають на великій відстані один від одного, але по швидкості передачі інформації *Gigabit Ethernet* істотно перевершує *FDDI*.

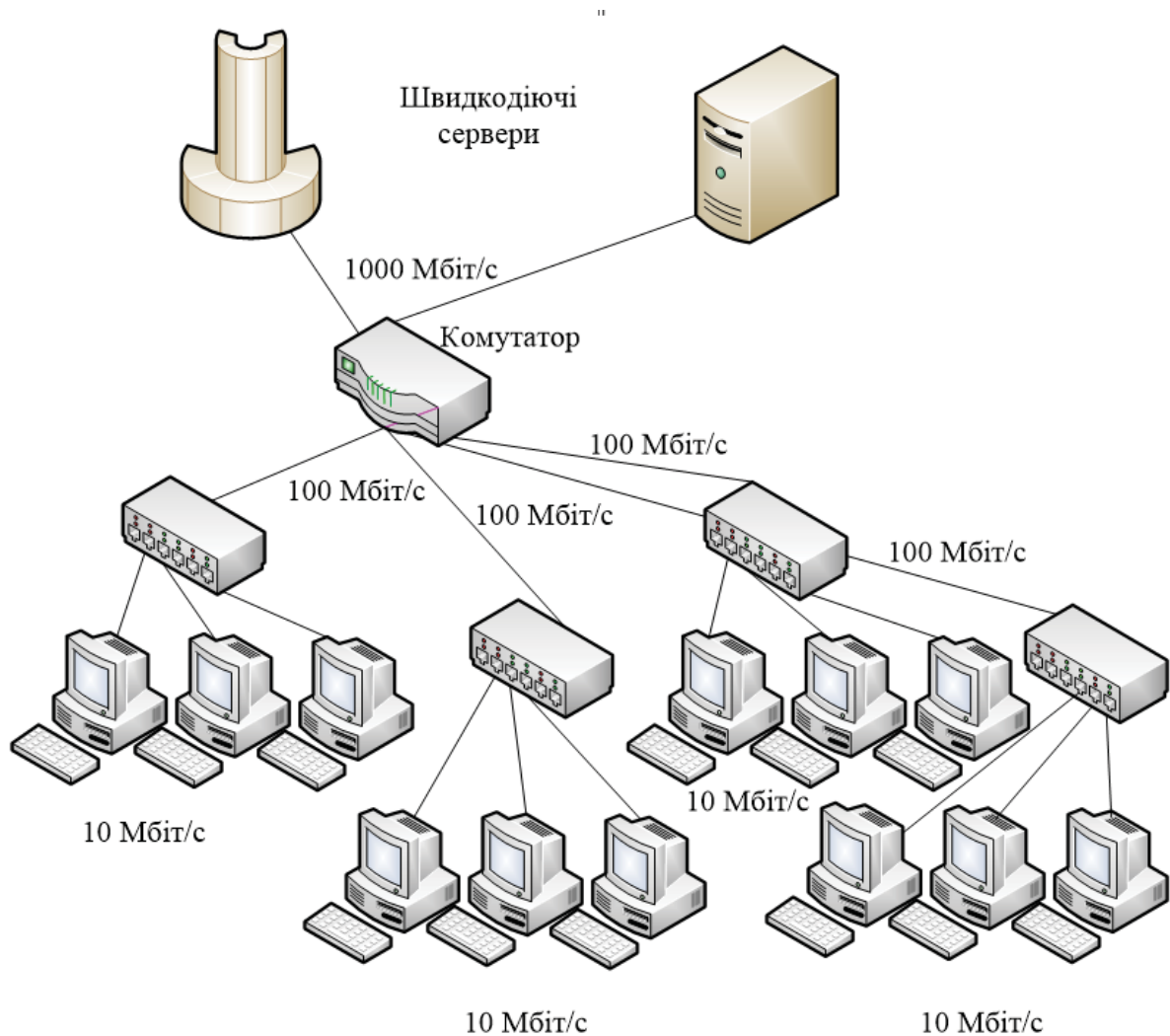


Рис. 4.31. Використання мережі Gigabit Ethernet для підключення швидкодіючих серверів

Але навіть мережа *Gigabit Ethernet* не може вирішити деяких завдань. Уже пропонується й 10-гігабітна версія Ethernet, називана *10Gigabit Ethernet* (стандарт IEEE 802.3ae, прийнятий в 2002 році). Вона принципово відрізняється від попередніх версій. Як *середовище передачі* використовується винятково оптоволоконний кабель. Електричний кабель може іноді застосовуватися тільки для зв'язку на короткі відстані (порядку

10 м). Режим обміну – повнодуплексний. *Формат кадру* Ethernet колишній. Це, напевно, єдине, що залишається від стандарту Ethernet (IEEE 802.3).

Технологія Gigabit Ethernet дозволила забезпечити прийнятий діаметр мережі 200 м при використанні концентраторів, досягнути швидкості передачі інформації 1000 Мбіт/с на основних типах кабелів і використовувати виту пару.

Для збільшення діаметрів мережі в технології Gigabit Ethernet збільшений мінімальний розмір кадру до 512 байт або 4096 біт (для технологій Ethernet і Fast Ethernet ця величина мала значення 64 байт або 512 біт).

При передачі інформації із швидкістю 1000 Мбіт/с по оптоволоконному кабелю величина подвоєної затримки на 1 м складає 10 bt. Пара мережевих адаптерів вносить затримку при подвійному обороті рівну 1000 bt. Півторювач вносить затримку, складову також 1000 bt. Якщо мережа з 1 повторювачем матиме діаметр 200 м, то час подвійного обороту складе $PDV = 10 \cdot 200 + 1000 + 1000 = 4000 \text{ bt} < 4096 \text{ bt}$.

Таким чином, за рахунок збільшення мінімального розміру кадру мережа технології Gigabit Ethernet може мати діаметр до 200 м.

При передачі коротких повідомлень в Gigabit Ethernet одному комп'ютеру дозволено передавати декілька кадрів підряд, проте, загальна довжина інформаційного блоку не повинна перевищувати 8192 байти. Таке збільшення кадру трохи затримує доступ інших комп'ютерів до середовища передачі, але при швидкості 1000 Мбіт/с ця затримка не дуже помітна.

Завдання досягнення швидкості передачі інформації 1000 Мбіт/с в мережах Gigabit Ethernet розв'язується шляхом використання наступних типів фізичного середовища:

- 1) багатомодового волоконно-оптичного кабелю;
- 2) одномодового волоконно-оптичного кабелю;
- 3) подвійного коаксіального кабелю (Twiax);
- 4) витої пари категорії 5.

Для багатомодового оптоволоконного кабелю, що використовується в мережах Gigabit Ethernet, визначені специфікації 1000Base-SX і 1000Base-FX.

Специфікація 1000Base-SX припускає використання оптоволоконна, що працює з сигналами з довжиною хвилі 850 нм (S означає Short Wavelength, тобто коротка хвиля). Відповідно до даної специфікації для кабелю 62,5 мкм MMF гранична довжина оптоволоконного сегменту складає 220 м, а для кабелю 50 мкм MMF – 500 м. Ці максимальні значення можуть досягатися тільки для повнодуплексної передачі даних. Для напівдуплексної передачі

максимальні значення сегментів оптоволоконного кабелю завжди повинні бути менше 100 м.

Відповідно до специфікації 1000Base-LX використовується оптоволоконний кабель, по якому передаються сигнали, що мають довжину хвилі 1300 нм (L означає Long Wavelength, тобто довга хвиля). Для багатомодового волокна гранична довжина сегменту 1000Base-LX складає 550 м.

Таким чином, технологія Gigabit Ethernet є завершеною та перевіреною на практиці технологією, яка дозволяє отримати високи показники пропускної здатності для мереж Ethernet при вартості обладнання істотно нижче ніж обладнання мереж ATM, FDDI і т.д. Цей факт дозволив зайняти центральне місце серед технологій побудови сучасних комп'ютерних мереж.

4.6. Технологія Wi-Fi

З кінця 90-х років 20 століття спостерігається справжній бум бездротових локальних мереж (WLAN – Wireless LAN) [17; 26; 43]. Це пов'язано в першу чергу з успіхами технології та з тими зручностями, які здатні надати бездротові мережі.

В 1997 році був прийнятий стандарт для бездротових мереж IEEE 802.11. Зараз цей стандарт активно розвивається та містить у собі вже декілька розділів, у тому числі три локальні мережі (802.11a, 802.11b і 802.11g). Стандарт містить наступні специфікації:

- 802.11 – первісний стандарт WLAN. Підтримує передачу даних зі швидкостями від 1 до 2 Мбіт/с.

- 802.11a – високошвидкісний стандарт WLAN для частоти 5 ГГц. Підтримує швидкість передачі даних 54 Мбіт/с.

- 802.11b – стандарт WLAN для частоти 2,4 ГГц. Підтримує швидкість передачі даних 11 Мбіт/с.

- 802.11e – встановлює вимоги якості запиту, необхідні для всіх радіо інтерфейсів IEEE WLAN.

- 802.11f – описує порядок зв'язку між рівнозначними точками доступу.

- 802.11g – встановлює додаткову техніку модуляції для частоти 2,4 ГГц. Призначений для забезпечення швидкостей передачі даних до 54 Мбіт/с.

- v802.11h – описує керування спектром частоти 5 ГГц для використання в Європі і Азії.

– 802.11i – виправляє існуючі проблеми безпеки в галузях автентифікації і протоколів шифрування.

Розробкою й підтримкою стандарту IEEE 802.11 займається комітет Wi-Fi Alliance. Термін Wi-Fi (wireless fidelity) використовується як загальне ім'я для стандартів 802.11a та 802.11b, а також всіх наступних, що відносяться до бездротових локальних мереж (WLAN).

4.6.1. Фізичний рівень протоколів IEEE 802.11

Стандарт IEEE 802.11, розробка якого була завершена у 1997 р., є базовим стандартом і визначає протоколи, необхідні для організації бездротових локальних мереж (Wireless Local Area Network, WLAN). Основні з них – протокол управління доступом до середовища MAC (Medium Access Control – нижній підрівень канального рівня) і протокол PHY передачі сигналів у фізичному середовищі. У якості останньої допускається використання радіохвиль і інфрачервоного випромінювання.

Стандартом IEEE 802.11 визначений єдиний підрівень MAC, взаємодіючий із трьома типами протоколів фізичного рівня, що відповідають різним технологіям передачі сигналів – по радіоканалах у діапазоні 2,4 ГГц із широкополосною модуляцією із прямим розширенням спектру (Direct Sequence Spread Spectrum, DSSS) і перескоком частоти (FHSS), а також за допомогою інфрачервоного випромінювання. Специфікаціями стандарту передбачені два значення швидкості передачі даних – 1 і 2 Мбіт/с.

У порівнянні із дротовими локальними мережами Ethernet можливості підрівня MAC розширені за рахунок включення в нього ряду функцій, що зазвичай виконуються протоколами більш високого рівня, зокрема, процедур фрагментації й ретрансляції пакетів. Це викликано прагненням підвищити ефективну пропускну здатність системи завдяки зниженню накладних витрат на повторну передачу пакетів.

Управління енергоресурсами. Для економії енергоресурсів мобільних робочих станцій, використовуваних у бездротових локальних мережах, стандартом IEEE 802.11 передбачений механізм перемикання станцій у так званий пасивний режим з мінімальним споживанням потужності.

Архітектура і компоненти мережі. В основу стандарту IEEE 802.11 покладена сотова архітектура, причому мережа може складатися як з однієї, так і декількох ячеек. Кожна сота управляється базовою станцією, що має назву точка доступу (Access Point, AP), що разом з перебуваючими у межах

радіуса її дії робочими станціями користувачів утворює базову зону обслуговування (Basic Service Set, BSS). Точки доступу багатосотової мережі взаємодіють між собою через розподільну систему (Distribution System, DS), що представляє собою еквівалент магістрального сегмента кабельних локальних мереж. Вся інфраструктура, що включає точку доступу і розподільну систему утворює розширену зону обслуговування (Extended Service Set).

Стандартом передбачений також односотовий варіант бездротної мережі, що може бути реалізований і без точки доступу, при цьому частина її функцій виконуються безпосередньо робочими станціями.

Роумінг. Для забезпечення переходу мобільних робочих станцій із зони дії однієї точки доступу до іншої в багатосотових системах передбачені спеціальні процедури сканування (активного й пасивного прослуховування ефіру) і приєднання (Association), однак строгих специфікацій по реалізації роумінгу стандарт IEEE 802.11 не передбачає.

Забезпечення безпеки. Для захисту WLAN стандартом IEEE 802.11 передбачений цілий комплекс мір безпеки передачі даних під загальною назвою Wired Equivalent Privacy, WEP. Він включає засоби протидії несанкціонованому доступу до мережі (механізми і процедури автентифікації), а також запобігання перехоплення інформації (шифрування).

Стандарт IEEE 802.11a

Є найбільш “широкополосним” із сімейства стандартів IEEE 802.11, передбачаючи швидкість передачі даних до 54 Мбіт/с (редакцією стандарту, затвердженої в 1999 р., визначені три обов’язкових швидкості – 6, 12 і 24 Мбіт/с і п’ять необов’язкових – 9, 18, 36, 48 і 54 Мбіт/с).

На відміну від базового стандарту, орієнтованого на область частот 2,4 ГГц, специфікаціями IEEE 802.11a передбачена робота в діапазоні 5 ГГц. Як метод модуляції сигналу обране ортогональне частотне мультиплексування (OFDM). Найбільш істотне розходження між цим методом і радіотехнологіями DSSS і FHSS полягає в тому, що OFDM припускає паралельну передачу корисного сигналу одночасно по декількох частотах діапазону, у той час як технології розширення спектра передають сигнали послідовно. В результаті підвищується пропускна здатність каналу і якість сигналу.

До недоліків IEEE 802.11a належать більш висока споживана потужність радіопередавачів для частот 5 ГГц, а так само менший радіус дії

(обладнання для 2,4 ГГц може працювати на відстані до 300м, а для 5 ГГц - близько 100м).

Стандарт IEEE 802.11b

Завдяки високій швидкості передачі даних (до 11 Мбіт/с), практично рівної пропускної здатності звичайних дротових локальних мереж Ethernet, а також орієнтації на “освоєний” діапазон 2,4 ГГц, цей стандарт завоював найбільшу популярність у виробників обладнання для бездротових мереж.

В остаточній редакції стандарт IEEE 802.11b, відомий також як Wi-Fi (Wireless Fidelity), був прийнятий в 1999 р. У якості базової радіотехнології в ньому використовується метод DSSS з 8-розрядними послідовностями Уолша.

Оскільки обладнання, що працює на максимальній швидкості 11 Мбіт/с має менший радіус дії, ніж на більш низьких швидкостях, то стандартом 802.11b передбачене автоматичне зниження швидкості при погіршенні якості сигналу.

Як і у випадку базового стандарту IEEE 802.11, чіткі механізми роумінгу специфікаціями IEEE 802.11b не визначені.

Специфікація IEEE 802.11g

Специфікації IEEE 802.11g являють собою розвиток стандарту 802.11b і дозволяють підвищити швидкість передачі даних у бездротових локальних мережах до 22 Мбіт/с (і вище) завдяки використанню більш ефективної модуляції сигналу. Одним з достоїнств стандарту є зворотна сумісність із IEEE 802.11b.

Фізичний рівень протоколу 802.11

Огляд протоколів сімейства 802.11b/g доцільно почати саме із протоколу 802.11, що, хоча вже й не зустрічається в чистому виді, у той же час є прабатьком всіх інших протоколів. У стандарті 802.11, як і у всіх інших стандартах даного сімейства, передбачене використання частотного діапазону від 2400 до 2483,5 МГц, тобто частотний діапазон шириною 83,5 МГц, що розбитий на декілька частотних підканалів.

4.6.2. Канальний рівень протоколів IEEE802.11.

Технологія колективного доступу в дротових мережах

На фізичному рівні сімейства протоколів IEEE 802.11 [17; 43; 45] визначаються механізми, які використовуються для перетворення даних, для забезпечення необхідної швидкості передачі залежно від середовища

передачі даних. Таким чином, фізичний рівень визначає методи кодування/декодування і модуляції/демодуляції сигналу при його передачі і прийомі.

У той же час такі питання, як регулювання спільного використання середовища передачі даних, визначаються на більш високому рівні – рівні доступу до середовища передачі даних. Цей рівень називають MAC-рівнем (Media Access Control). Саме на MAC-рівні встановлюються правила спільного використання середовища передачі даних одночасно декількома вузлами бездротової мережі.

На MAC-рівні визначаються два основних типи архітектури дротових мереж – Ad Hoc і Infrastructure Mode.

Режим Ad Hoc

У режимі Ad Hoc (рис. 4.32), що називають також Independent Basic Service Set (IBSS) або режимом Peer to Peer (точка-точка), станції безпосередньо взаємодіють один з одним. Для цього режиму потрібний мінімум обладнання: кожна станція повинна бути оснащена бездротовим адаптером. При такій конфігурації не потрібно створення мережної інфраструктури. Основним недоліком режиму Ad Hoc є обмежений діапазон дії можливої мережі.

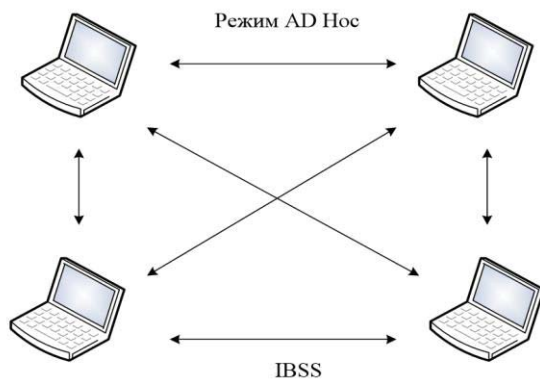


Рис. 4.32. Режим функціонування Ad Hoc

Режим Infrastructure Mode

У режимі Infrastructure Mode (рис. 4.33) станції взаємодіють один з одним не прямо, а через точку доступу (Access Point), що виконує в бездротовій мережі роль своєрідного концентратора (аналогічно тому, як це відбувається в традиційних кабельних мережах).

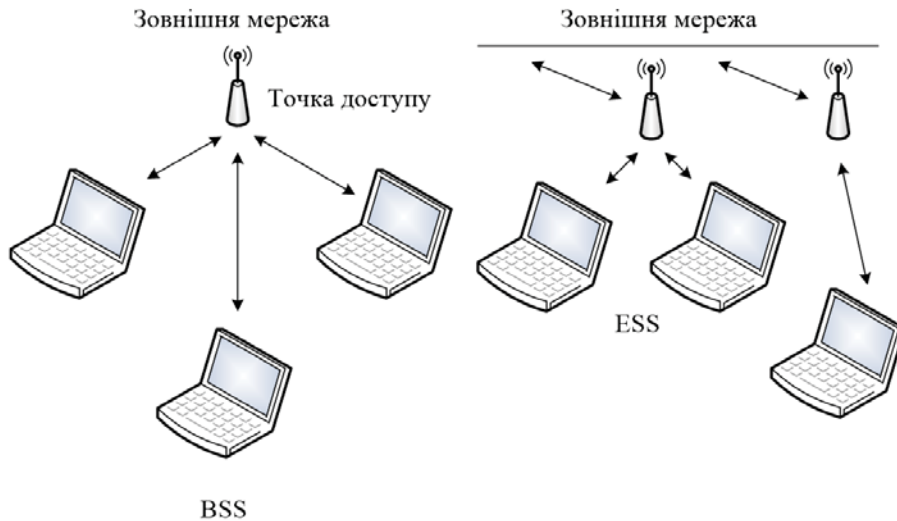


Рис. 4.33. Режим функціонування Infrastructure Mode

Розглядають два режими взаємодії із точками доступу – BSS (Basic Service Set) і ESS (Extended Service Set). У режимі BSS всі станції зв'язуються між собою тільки через точку доступу, що може виконувати також роль мосту до зовнішньої мережі. У розширеному режимі ESS існує інфраструктура декількох мереж BSS, причому самі точки доступу взаємодіють одна з одною, що дозволяє передавати трафік від однієї BSS до іншої.

Крім двох різних режимів функціонування дротових мереж на MAC-рівні визначаються правила колективного доступу до середовища передачі даних. Необхідність існування таких регламентуючих правил цілком очевидна. Якщо кожний вузол бездротової мережі, не дотримуючи ніяких правил, став би передавати дані в ефір, то в результаті інтерференції декількох таких сигналів вузли, яким призначалася відправлена інформація, не змогли б не тільки її одержати, але і зрозуміти, що дана інформація адресована їм. Саме тому, необхідне існування твердих регламентуючих правил, які визначали б колективний доступ до середовища передачі даних. На MAC-рівні протоколу IEEE 802.11 визначаються два типи колективного доступу до середовища передачі даних: функція розподіленої координації (Distributed Coordination Function, DCF) і функція централізованої координації (Point Coordination function, PCF).

Контрольні запитання

1. Поясніть різницю між розширюємістю та масштабуємістю на прикладі технології Ethernet.
2. Що таке колізія?
3. У чому складаються функції преамбули та початкового обмежувача кадра в Ethernet?
4. Чим пояснюється, що мінімальний розмір кадра в стандарті 10-Base-5 складає 64 байт?
5. Чому стандарти 10-Base-T та 10-Base-FL/FB витиснули стандарти Ethernet на коаксіальному кабелі?
6. За рахунок чого мережа Token Ring не губить зв'язок при відключенні одного з комп'ютерів, який входить у кільце?
7. З яких умов обирається максимальний час обертання токєну у мережі Token Ring?
8. Визначте максимально допустимий розмір поля даних для технології Token Ring?
9. Які елементи мережі FDDI забезпечують відмово стійкість?
10. До яких наслідків може призвести обрив кабелю у двох місцях кільця FDDI?
11. У чому полягає схожість та відмінність технологій FDDI та Token Ring?
12. Чому дорівнює мінімальний між кадровий інтервал (IPG) в технології Gigabit Ethernet?
13. Які методи кодування сигналів застосовуються у IEEE 802.11?
14. Яким чином викриває колізії рівень MAC в мережах 802.11?

РОЗДІЛ 5. ХАРАКТЕРИСТИКИ МЕРЕЖНОГО РІВНЯ

Мережний рівень, або 3-й рівень еталонної моделі OSI, надає послуги, що дозволяють кінцевим пристроям обмінюватися даними через мережі. IP версії 4 (IPv4) та IP версії 6 (IPv6) є основними протоколами зв'язку мережного рівня. Інші протоколи мережного рівня включають протоколи маршрутизації, такі як Open Shortest Path First (OSPF) і протоколи обміну повідомленнями, такі як Internet Control Message Protocol (ICMP).

Для забезпечення можливості наскрізного зв'язку через межі мереж, протоколи мережного рівня виконують чотири основні операції:

- *Адресація кінцевих пристроїв* – кінцеві пристрої повинні бути налаштовані з унікальною IP-адресою для ідентифікації в мережі.
- *Інкапсуляція* – мережний рівень інкапсулює блок даних протоколу (PDU, Protocol Data Unit) транспортного рівня у пакет. Процес інкапсуляції додає інформацію IP-заголовка, наприклад IP-адресу вихідного хоста (відправника) і хоста призначення (отримувача). Процес інкапсуляції виконується джерелом IP-пакета.
- *Маршрутизація* – мережний рівень забезпечує спрямування пакетів на хост призначення в іншій мережі. Для переміщення в інші мережі пакет повинен бути оброблений маршрутизатором. Роль маршрутизатора полягає в тому, щоб вибрати оптимальний шлях і спрямувати пакети до хоста призначення. Цей процес називається маршрутизацією. Пакет може переходити через багато маршрутизаторів поки досягне хоста призначення. Кожен маршрутизатор, який пакет перетинає, щоб дістатися до хоста призначення, називається переходом.
- *Деінкапсуляція* – коли пакет надходить на мережний рівень хоста призначення, хост перевіряє IP-заголовок пакета. Якщо IP-адреса призначення в заголовку відповідає його власній IP-адресі, IP-заголовок видаляється з пакета. Після того, як пакет деінкапсульований на мережному рівні, результуючий PDU 4-го Рівня передається до відповідної служби на транспортному рівні. Процес деінкапсуляції виконується кінцевим хостом IP-пакета.

На відміну від транспортного рівня (4-го рівня OSI), який керує передачею даних між процесами, запущеними на кожному хості, протоколи зв'язку мережного рівня (тобто IPv4 та IPv6) визначають структуру пакетів і їх обробку для передачі даних з одного хоста на інший. Функціонування без

урахування даних, що передаються в кожному пакеті, дозволяє мережному рівню передавати пакети для кількох типів зв'язку між кількома хостами.

IP-протокол інкапсулює сегмент транспортного рівня (наступний над мережним рівнем) або інші дані, шляхом додавання IP-заголовка. IP-заголовки використовуються для доставки пакета до хоста призначення.

IP-заголовки переглядаються пристроями 3-го Рівня (тобто маршрутизаторами та комутаторами Рівня 3) під час руху через мережу до місця призначення. Важливо відзначити, що інформація про IP-адресацію залишається незмінною з моменту виходу пакета з вихідного хоста, і доки він не надходить на хост призначення, за винятком випадків її перетворення пристроєм, що здійснює перетворення мережних адрес (NAT, Network Address Translation) для IPv4.

Маршрутизатори реалізують протоколи маршрутизації для спрямування пакетів між мережами. Проміжні пристрої, що здійснюють маршрутизацію, перевіряють адресацію мережного рівня в заголовку пакета. У всіх випадках частина даних пакета, тобто інкапсульований PDU транспортного рівня або інші дані, залишається незмінною під час процесів мережного рівня.

5.1. Характеристики IP-протоколу

Протокол IP проектувався як протокол з низькими накладними витратами. Він забезпечує лише функції, необхідні для доставки пакета з вихідного хоста на хост-отримувач через взаємопов'язану систему мереж. Протокол не призначений для відстеження та керування потоком пакетів. Ці функції, за необхідності, виконуються іншими протоколами - переважно протоколом TCP на Рівні 4.

Основні характеристики протоколу IP:

- *Не орієнтований на з'єднання (Connectionless)* – Перед надсиланням пакетів даних не встановлюється канал зв'язку з адресатом. IP-протокол не орієнтований на з'єднання, а це означає, що перед передачею даних не створюється виділений наскрізний канал.
- *Негарантована доставка (Best Effort)* – IP по суті є ненадійним, оскільки не гарантує доставку пакетів. IP також не потребує додаткових полів у заголовку для підтримки встановленого з'єднання. Це значно зменшує накладні витрати IP.

- *Незалежний від середовища передавання даних (Media Independent)* – Функціонує незалежно від середовища передавання даних (тобто мідний чи волоконно-оптичний кабель або бездротове з'єднання). Ненадійність означає, що IP не має можливості керувати доставкою та повторно надсилати недоставлені або пошкоджені пакети. Це тому, що хоча IP-пакети відправляються з інформацією про місце доставки, вони не містять інформації, обробка якої дозволила б інформувати відправника про те, чи була доставка успішною. Пакети можуть надходити до місця призначення пошкодженими, невпорядкованими, або взагалі будуть втрачені. IP не надає можливості для повторного передавання пакетів у разі виникнення помилок.

Якщо пакети доставлені в іншому порядку, ніж були відправлені, або деякі з них були втрачені, то вирішувати ці проблеми повинні сервіси вищого рівня. Це дозволяє протоколу IP функціонувати дуже ефективно. В стеку протоколів TCP/IP за надійність відповідає протокол TCP транспортного рівня.

IP працює незалежно від середовища, в якому передаються дані на нижчих рівнях стеку протоколів.

Канальний рівень повинен прийняти IP-пакет і підготувати його до передачі через середовище передавання даних. Це означає, що транспортування IP-пакетів не обмежується певним комунікаційним середовищем.

5.2. Пакет IPv4

IPv4 є одним з основних протоколів зв'язку мережного рівня. Заголовок пакета IPv4 використовується для забезпечення доставки цього пакета до наступної зупинки на шляху до кінцевого пристрою.

Заголовок пакета IPv4 складається з декількох полів, що містять важливу інформацію про пакет. Ці поля містять двійкові числа, які аналізуються процесом Рівня 3 (рис. 5.1).

Версія – Містить 4-бітне двійкове значення, що визначає версію IP-пакета. Для пакетів IPv4 у цьому полі завжди вказано значення 0100.

Диференційовані сервіси (DS) – Поле, яке раніше називалося "Тип сервісу" (ToS); DS – це 8-бітне поле, що використовується для визначення пріоритету кожного пакета. 6 найважливіших бітів поля диференційованих послуг (DSCP) і останні 2 біти – це біти явного повідомлення про затори (ECN).



Рис. 5.1. Поля заголовку пакета IPv4

Час існування (Time-to-Live, TTL). Містить 8-бітове двійкове значення, що використовується для обмеження часу існування пакета. Відправник пакета встановлює початкове значення часу існування (TTL), яке зменшується на одиницю щоразу під час обробки пакета маршрутизатором. Якщо значення в полі TTL зменшується до нуля, маршрутизатор відкидає пакет і відправляє на IP-адресу джерела повідомлення про перевищення часу протоколу ICMP (управління повідомленнями в мережі).

Поле *Протокол* використовується для визначення протоколу наступного рівня. Це 8-бітове двійкове значення, що вказує тип корисного навантаження даних, які переносить пакет, що дозволяє мережевому рівню пересилати дані на відповідний протокол вищого рівня. Зазвичай використовуються значення ICMP (1), TCP (6) і UDP (17).

IPv4-адреса джерела містить 32-бітове двійкове значення, яке представляє IPv4-адресу джерела пакета. IPv4-адреса джерела – це завжди індивідуальна адреса.

IPv4-адреса призначення містить 32-бітове двійкове значення, яке представляє IPv4-адресу призначення пакета. IPv4-адреса призначення – одноадресна розсилка, багатоадресна розсилка, або широкомовна адреса [8].

5.3. Пакет IPv6

На початку 1990-х років Інженерна група з розвитку Інтернету (IETF, Internet Engineering Task Force), стурбована проблемами з IPv4, почала

шукати заміну. Результатом стала розробка IP версії 6 (IPv6). IPv6 долає обмеження IPv4 і значно розширює можливості за рахунок функцій, що краще відповідають поточним і передбачуваним вимогам мережі.

Покращення, які забезпечує IPv6 включають наступні:

- *Збільшений адресний простір* – IPv6-адреси базуються на 128-бітній ієрархічній адресації на відміну від IPv4 з 32 бітами.
- *Покращена обробка пакетів* – заголовок IPv6 був спрощений: він містить меншу кількість полів.
- *Позбавляє від необхідності використання NAT* – при такій великій кількості загальнодоступних IPv6-адрес, NAT між приватною і загальнодоступною адресами IPv4 не потрібен. Це дозволяє уникнути деяких проблем, спричинених NAT, з якими стикаються додатки, що потребують наскрізного підключення.

32-розрядний адресний простір IPv4 забезпечує приблизно 4 294 967 296 унікальних адрес. Адресний простір IPv6 надає 340 282 366 920 938 463 463 374 607 431 768 211 456 або 340 ундецильйонів (10^{36}) адрес.

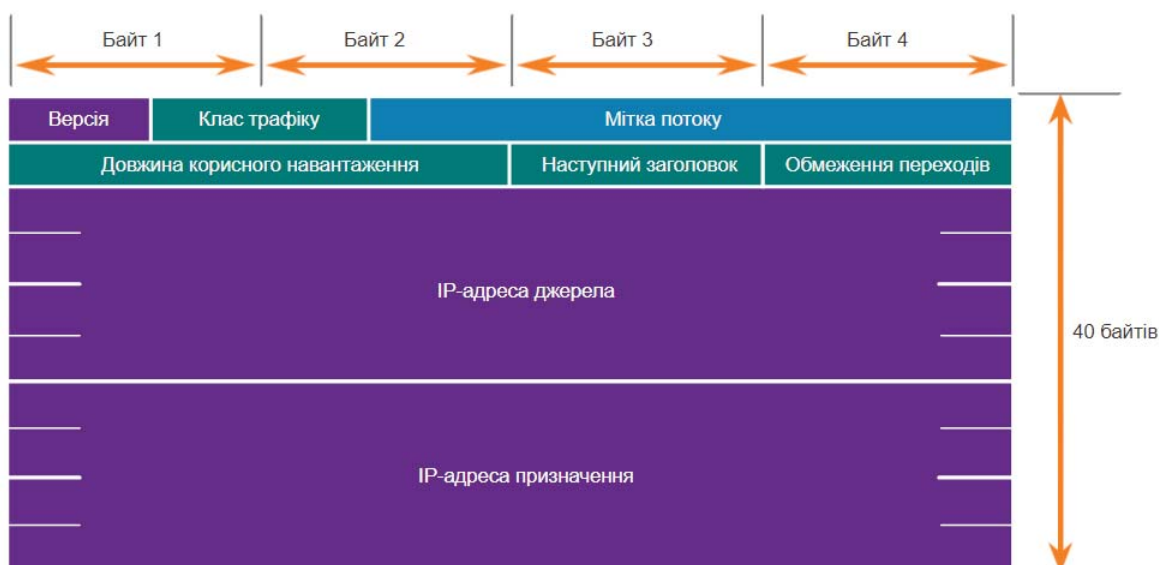


Рис. 5.2. Поля заголовку пакета IPv6

Поля в заголовку пакета IPv6:

Версія. Це поле містить 4-бітне двійкове значення, яке визначає версію IP-пакета. Для пакетів IPv6 у цьому полі завжди вказано значення 0110.

Клас трафіку. Це 8-бітне поле, що відповідає полю "Диференційовані сервіси (DS)" у заголовку IPv4.

Мітка потоку. Це 20-бітове поле вказує на те, що всім пакетам з однаковими мітками потоку призначається однаковий тип обробки маршрутизаторами.

Довжина корисного навантаження. Це 16-бітове поле вказує довжину блоку даних або корисного навантаження пакета IPv6.

Наступний заголовок. Це 8-бітове поле, що відповідає полю "Протокол" у заголовку IPv4. Воно вказує тип корисного навантаження даних, які переносить пакет, що дозволяє мережевому рівню пересилати дані на відповідний протокол вищого рівня.

Межа переходу. Це 8-бітове поле, що замінює поле "Час існування" (TTL) в IPv4. Це значення зменшується на одиницю кожним маршрутизатором, що пересилає пакет. Коли лічильник досягає значення 0, пакет відкидається, і на вузол-відправник пересилається повідомлення ICMPv6, яке означає, що пакет не досягнув свого призначення, оскільки було перевищено межу переходів.

IPv6-адреса джерела. Це 128-бітове поле, що визначає IPv6-адресу приймаючого вузла.

IPv6-адреса призначення. Це 128-бітове поле, що визначає IPv6-адресу приймаючого вузла.

Пакет IPv6 також може включати заголовки розширень (extension headers, EH), які надають додаткову інформацію мережного рівня. Заголовки розширень є необов'язковими і розміщуються між заголовком IPv6 та корисним завантаженням. EH використовуються для фрагментації, безпеки, підтримки мобільності тощо.

На відміну від IPv4, маршрутизатори не фрагментують IPv6-пакети при передаванні.

5.4. Адресація IPv4

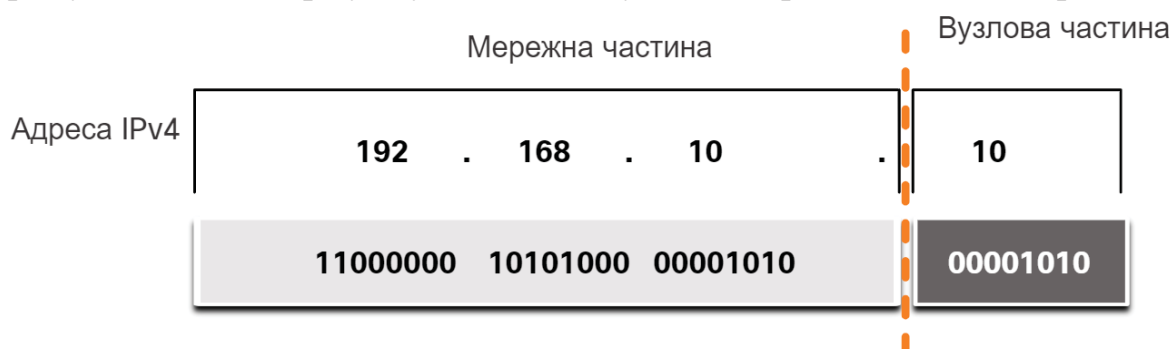
5.4.1. Мережева та вузлова частина

Адреса IPv4 – це 32-розрядна ієрархічна адреса, яка складається з мережної частини та вузлової частини.

Біти в мережній частині адреси повинні бути однаковими для всіх пристроїв, які знаходяться в одній мережі. Біти вузлової частини адреси повинні бути унікальними для ідентифікації конкретного вузла в мережі.

Якщо два вузли мають однакову бітову комбінацію в певній мережній частині 32-бітного потоку, то ці два вузли знаходяться в одній і тій же мережі.

Але як вузли визначають, яка частина 32-бітного потоку ідентифікує мережу, а яка ідентифікує вузол? У цьому полягає роль маски підмережі.



- *Адреса IPv4* – це унікальна IPv4-адреса вузла.
- *Маску підмережа* – яка використовується для визначення мережної/вузлової частини IPv4-адреси.

Маска підмережі IPv4 використовується для розмежування мережної частини від вузлової частини адреси IPv4. Коли пристрою призначається адреса IPv4, маска підмережі використовується для визначення мережної адреси пристрою. Адреса мережі представляє всі пристрої в одній мережі.

Подання мережних і вузлових адрес у вигляді маски підмережі в десятковому форматі розділеному крапками може стати громіздким. Існує альтернативний, більш простий, спосіб визначення маски підмережі, який називається довжиною префікса.

Довжина префікса – це кількість бітів, встановлених в одиницю (1) у масці підмережі. Вона позначається скісною рисою («/»), за якою вказується кількість бітів, встановлених в 1. Отже, потрібно підрахувати кількість бітів у масці підмережі й поставити перед цим значенням скісну риску.

Під час подання адреси IPv4 з використанням довжини префікса записується IPv4-адреса, а потім довжина префікса без пробілів. Наприклад, 192.168.10.10 255.255.255.0 буде записано як 192.168.10.10/24.

Щоб визначити мережну IPv4-адресу вузла для IPv4-адреси та маски підмережі побітово виконується логічна операція І. У результаті виконання логічної операції І (AND) над адресою та маскою підмережі отримаємо адресу мережі (рис. 5.3).

- *IPv4-адреса вузла (192.168.10.10)* – IPv4-адреса вузла в десятковому і двійковому форматах розділених крапками.

- *Маска підмережі (255.255.255.0)* – Маска підмережі вузла в десятковому і двійковому форматах розділених крапками.
- *Мережна адреса (192.168.10.0)* – логічна операція І між IPv4-адресою та маскою підмережі призводить до отримання мережної адреси IPv4, показаної у десятковому і двійковому форматах розділених крапками.

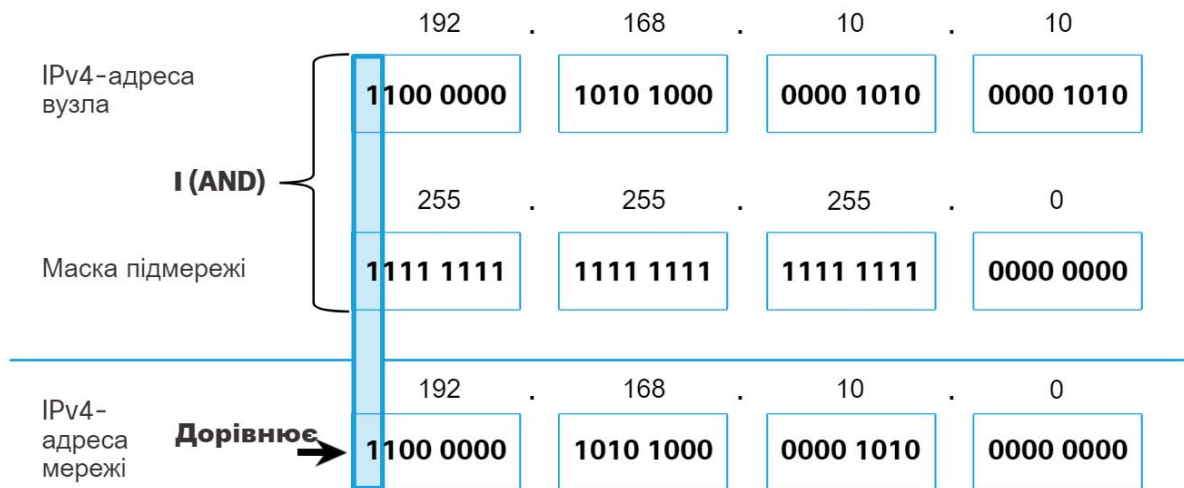


Рис. 5.3. Визначення адреси мережі та адреси вузла

Операція І між адресою вузла IPv4 і маскою підмережі призводить до отримання мережної IPv4-адреси для цього вузла. У цьому прикладі операція І між адресою вузла 192.168.10.10 і маскою підмережі 255.255.255.0 (/24), призводить до мережної IPv4-адреси 192.168.10.0/24. Це важлива операція IPv4, оскільки вона повідомляє вузлу, до якої мережі він належить.

5.4.2. Адреса мережі, адреса вузла та широкомовна адреса

У межах кожної мережі є три типи IP-адрес:

- Адреса мережі
- Адреса вузла
- Широкомовна адреса

Адреса мережі

Адреса мережі – це адреса, яка представляє конкретну мережу. Пристрій належить до цієї мережі, якщо він відповідає трьом критеріям:

- Він має ту ж маску підмережі, що і адреса мережі.
- Він має ті ж мережні біти, що і адреса мережі, як зазначено в масці підмережі.

- Він розміщений у тому ж широкомовному домені, що й інші вузли з тією ж адресою мережі.

Вузол визначає свою мережну адресу, виконуючи операцію І між адресою IPv4 і маскою підмережі.

Адреса вузла

Адреси вузлів – це адреси, які можуть бути призначені пристрою, наприклад, хост-комп'ютер, ноутбук, смарт-телефон, веб-камера, принтер, маршрутизатор тощо. Вузлова частина адреси - це біти, позначені 0 бітами в масці підмережі. Адреси вузлів можуть мати будь-яку комбінацію бітів у вузловій частині, за винятком усіх 0 бітів (це буде мережна адреса) або усіх 1 бітів (це буде широкомовна адреса).

Всі пристрої в одній мережі, повинні мати однакову маску підмережі та однакові мережні біти. Тільки біти вузла будуть відрізнятися і повинні бути унікальними.

Зверніть увагу, що в таблиці є перша та остання адреса вузла:

- *Перша адреса вузла* – У першого вузла в мережі є всі 0 біти з останнім (самим правим) бітом 1. Наприклад 192.168.10.1/24.
- *Остання адреса вузла* – У останнього вузла в мережі є всі 1 біти з останнім (самим правим) бітом 0. Наприклад 192.168.10.254/24.

Будь-які адреси між 192.168.10.1/24 до 192.168.10.254/24 включно можна призначати пристрою в мережі.

Таблиця 5.1.

Адреса мережі, адреса вузла та широкомовна адреса

Мережна частина	Вузлова частина	Біти вузла	
Маска підмережі 255.255.255.0 або /24	255 255 255 11111111 11111111 11111111	0 00000000	
Адреса мережі 192.168.10.0 або /24	192 168 10 11000000 10100000 00001010	0 00000000	Всі 0
Перша адреса 192.168.10.1 або /24	192 168 10 11000000 10100000 00001010	1 00000001	Всі 0 і 1

Мережна частина	Вузлова частина	Біти вузла	
Остання адреса 192.168.10.254 або /24	192 168 10 11000000 10100000 00001010	254 11111110	Всі 1 і 0
Широкомовна адреса 192.168.10.255 або /24	192 168 10 11000000 10100000 00001010	255 11111111	Всі 1

Широкомовна адреса

Широкомовна адреса - це адреса, яка використовується, коли потрібно охопити всі пристрої в мережі IPv4. Як показано в таблиці, широкомовна адреса має всі 1 біти в частині вузла, що визначається маскою підмережі. В даному прикладі мережна адреса 192.168.10.255/24. Широкомовну адресу не можна призначати пристрою.

5.5. Одноадресна, широкомовна та групова розсилки IPv4

5.5.1. Одноадресна розсилка

Одноадресна розсилка (Unicast) відноситься до одного пристрою, який надсилає повідомлення одному іншому пристрою в режимі зв'язку «один до одного».

Одноадресний пакет має IP-адресу призначення, яка є одноадресною адресою, яка переходить до одного одержувача. IP-адреса джерела може бути лише одноадресною адресою, тому що пакет може створюватися лише одним джерелом. Це не залежить від того, чи IP-адреса призначення є одноадресною, широкомовною або груповою (багатоадресною).

Одноадресні IPv4-адреси вузлів знаходяться в діапазоні адрес від 1.1.1.1 до 223.255.255.255. Однак в межах цього діапазону є багато адрес, які зарезервовані для спеціальних цілей.

5.5.2. Широкомовна розсилка

Широкомовна розсилка (Broadcast) пов'язана з пристроєм, який надсилає повідомлення на всі пристрої в мережі в режимі зв'язку «один до всіх».

Пакет широкомовної розсилки містить IPv4-адресу призначення, у вузловій частині якого присутні тільки одиниці (1) або 32 одиничні (1) біти.

IPv4 використовує широкомовні пакети. Однак, в IPv6 не має широкомовних пакетів.

Пакет широкомовної розсилки повинен оброблятися усіма пристроями в одному широкомовному домені. Широкомовний домен ідентифікує всі вузли в одному сегменті мережі. Широкомовна розсилка може бути двох типів: пряма (directed) або обмежена (limited). Пряма широкомовна розсилка відправляється усім вузлам у конкретній мережі. Наприклад, вузол у мережі 172.16.4.0/24 відправляє пакет на 172.16.4.255. Обмежена широкомовна розсилка відправляється на адресу 255.255.255.255. За замовчуванням маршрутизатори не пересилають широкомовні повідомлення (пакети).

Пакети широкомовної розсилки використовують ресурси в мережі та змушують кожного приймаючого вузла в мережі обробляти пакет. Тому, широкомовний трафік повинен бути обмежений, щоб він не впливав негативно на продуктивність мережі чи пристроїв. Оскільки маршрутизатори розділяють широкомовні домени, розподіл мереж може підвищити продуктивність мережі за рахунок усунення надмірного широкомовного трафіку.

Крім того, для широкомовної адреси 255.255.255.255 в кожній мережі є широкомовна IPv4-адреса. Пряма широкомовна розсилка використовує найвищу адресу в мережі, тобто адресу, де всі вузлові біти встановлені в 1. Наприклад, пряма широкомовна адреса для 192.168.1.0/24 - це 192.168.1.255. Ця адреса дозволяє взаємодіяти з усіма вузлами в цій мережі. Щоб надіслати дані всім вузлам в мережі, вузол може надіслати один пакет, який адресований широкомовній адресі мережі.

Пристрій, який безпосередньо не під'єднаний до мережі призначення, перенаправляє спрямовані широкомовні пакети з IP-адресою так само, як і одноадресні IP-пакети, призначені вузлу в цій мережі. Коли спрямований широкомовний пакет досягає маршрутизатора, який безпосередньо під'єднаний до мережі призначення, цей пакет передається у мережу призначення.

5.5.3. Групова розсилка

Групова розсилка (Multicast) зменшує трафік, дозволяючи вузлу надсилати один пакет обраній групі вузлів, які підписані на групову розсилку.

Пакет групової розсилки – це пакет з IP-адресою призначення, яка належить до адреси групової розсилки. Для групової розсилки в IPv4 зарезервовано діапазон адрес від 224.0.0.0 до 239.255.255.255.

Вузли, які отримують пакети, що належать до групової розсилки, називаються клієнтами групової розсилки (multicast clients). Клієнти групової розсилки використовують служби, які вимагає клієнтська програма, щоб підписатися на групу групових розсилок.

Кожна група групової розсилки представлена однією груповою IPv4-адресою призначення. Коли IPv4-вузол підписується на групову розсилку, вузол обробляє пакети, адресовані цією груповою розсилкою, та пакети, адресовані його унікальній індивідуальній адресі.

Протоколи маршрутизації, такі як OSPF, використовують групові передавання. Наприклад, маршрутизатори з підтримкою OSPF підтримують зв'язок між собою за допомогою зарезервованої OSPF групової адреси 224.0.0.5. Тільки пристрої, ввімкнені за допомогою OSPF, оброблятимуть ці пакети з IPv4-адресою призначення 224.0.0.5. Всі інші пристрої ігноруватимуть ці пакети.

5.6. Типи адрес IPv4

5.6.1. Публічні та приватні адреси IPv4

Так само, як існують різні способи передавання пакета IPv4, також існують різні типи адрес IPv4. Деякі адреси IPv4 не можна використовувати для виходу в Інтернет, а інші спеціально призначені для маршрутизації в Інтернеті. Деякі використовуються для того, щоб перевірити з'єднання, а інші призначаються самостійно. Як адміністратор мережі, ви зрештою будете дуже добре ознайомлені з типами адрес IPv4, але поки що вам слід принаймні знати, що вони собою представляють та коли їх використовувати.

Публічні адреси IPv4 – це адреси, які глобально маршрутизуються між маршрутизаторами постачальника послуг Інтернету (ISP, Internet Service Provider).

Публічні адреси IPv4 – це адреси, які глобально маршрутизуються між маршрутизаторами в Інтернеті. Публічні адреси IPv4 повинні бути унікальними.

Призначення IPv4- і IPv6-адрес регулюється Адміністрацією адресного простору Інтернету (IANA, Internet Assigned Numbers Authority). IANA керує

та розподіляє блоки IP-адрес до регіональних інтернет-реєстраторів (RIR, Regional Internet Registries).

Регіональні інтернет-реєстратори (RIR) відповідальні за розподіл IP-адрес між інтернет-провайдерами (ISP), які в свою чергу, надають блоки адрес IPv4 організаціям та меншим інтернет-провайдерам. Організації також можуть отримувати свої адреси безпосередньо від регіональних інтернет-реєстраторів (в залежності від правил конкретного RIR).

Однак не всі доступні IPv4-адреси можна використовувати в Інтернеті. Є блоки адрес, які називаються приватними адресами. Такі адреси більшість організацій використовують для призначення IPv4-адрес внутрішнім вузлам.

У середині 1990-х років із впровадженням Всесвітнього павутиння (WWW) через виснаження адресного простору IPv4 були введені приватні IPv4-адреси. Приватні IPv4-адреси не є унікальними і можуть використовуватися у будь-якій внутрішній мережі.

Таблиця 5.2.

Блоки приватних адрес:

<i>Адреса мережі та префікс</i>	<i>Діапазон приватних адрес RFC 1918</i>
10.0.0.0/8	10.0.0.0 - 10.255.255.255
172.16.0.0/12	172.16.0.0 - 172.31.255.255
192.168.0.0/16	192.168.0.0 - 192.168.255.255

Більшість внутрішніх мереж, від великих підприємств до домашніх мереж, використовують приватні адреси IPv4 для адресації всіх внутрішніх пристроїв (інтрамережі), включаючи вузли й маршрутизатори. Однак, приватні адреси не є глобально маршрутизованими.

Приватні IPv4-адреси та трансляція мережних адрес (NAT)

Перш ніж ISP перенаправлятиме цей пакет, він повинен перевести IPv4-адресу джерела, яка є приватною адресою, на публічну IPv4-адресу за допомогою трансляції мережних адрес (NAT, Network Address Translation). NAT здійснює перетворення між приватними та публічними IPv4-адресами. Маршрутизатор зазвичай з'єднує внутрішню мережу з мережею провайдера послуг Інтернету (ISP). Приватні адреси IPv4 в інтрамережі організації будуть перекладені на публічні адреси IPv4 перед маршрутизацією в Інтернет.

Незважаючи на те, що пристрій з приватною адресою IPv4 не є доступним з іншого пристрою через Інтернет, IETF не розглядає приватні адреси IPv4 або NAT в якості ефективних заходів безпеки.

Організації, які мають ресурси, доступні в Інтернеті, наприклад веб-сервер, також матимуть пристрої, які мають публічні адреси IPv4. Як показано на рисунку 5.2, ця частина мережі відома як демілітаризована зона (DMZ, demilitarized zone). Маршрутизатор не тільки виконує маршрутизацію, він також виконує NAT і виступає в якості брандмауера для забезпечення безпеки.

Схема являє собою топологію мережі, у центрі якої є маршрутизатор з трьома з'єднаннями: до Інтрамережі (Intranet) компанії, до DMZ і до Інтернету. Зліва знаходиться Інтрамережа з пристроями, що використовують приватні адреси IPv4. У верхній частині знаходиться DMZ з двома серверами, що використовують публічні адреси IPv4. Праворуч – Інтернет-хмара (Internet cloud). Маршрутизатор діє як брандмауер і виконує NAT.

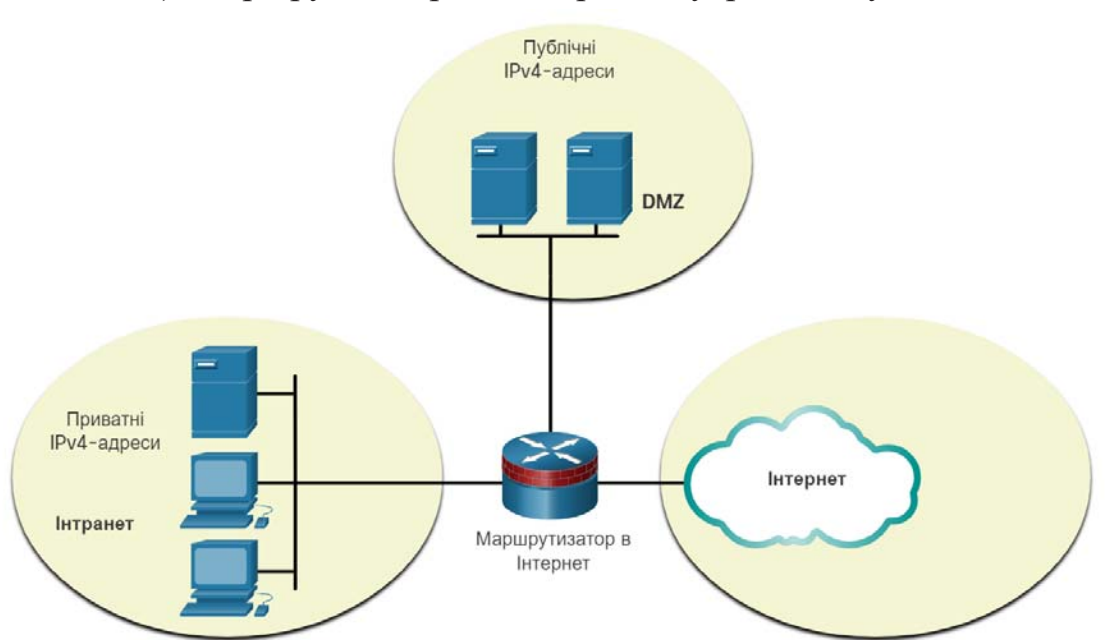


Рис. 5.2. Топологія мережі

5.6.2. IPv4-адреси спеціального призначення

Деякі адреси (наприклад, мережна і ширококомовна) не можуть бути призначені вузлам. Також є спеціальні адреси, які можна призначати вузлам, але з обмеженнями на те, як ці вузли можуть взаємодіяти в мережі.

Адреси зворотного зв'язку

Адреси loopback (127.0.0.0 /8 або 127.0.0.1 до 127.255.255.254) частіше ідентифікуються як 127.0.0.1 – це спеціальна адреса, яку використовують вузли, щоб спрямовувати трафік на себе. Наприклад, вони можуть використовуватися вузлом, щоб перевірити працездатність TCP/IP.

Локальні адреси каналу

Локальні адреси каналу (Link-local) (169.254.0.0 /16 або 169.254.0.1 до 169.254.255.254) більш відомі як автоматична приватна IP-адресація (APIPA, Automatic Private IP Addressing) або самопризначені адреси. Вони використовуються Windows DHCP-клієнтом для самостійної конфігурації у випадку, якщо ні один DHCP-сервер не доступний. Локальні адреси каналу можуть використовуватися в одноранговому зв'язку, але зазвичай не використовуються для цих цілей.

Застаріла класова адресація

У 1981 році IPv4-адреси були призначені за допомогою класової адресації, визначеної в RFC 790 (Призначення адрес). Клієнтам виділялася адреса мережі на основі одного з трьох класів А, В або С. Відповідно до стандарту RFC одноадресні діапазони поділяються на наступні класи:

- *Клас А (0.0.0.0/8 to 127.0.0.0/8)* – Розроблений для підтримки надзвичайно великих мереж з більш ніж 16 мільйонами адрес вузлів. Клас А використовував фіксований префікс /8 із першим октетом для позначення адреси мережі, а інші три октети - як другий вузлів (понад 16 мільйонів адрес вузлів у мережі).
- *Клас В (128.0.0.0 /16 - 191.255.0.0 /16)* – Розроблений для підтримки потреб середніх і великих мереж, що містять приблизно 65 000 вузлів. Клас В використовував фіксований префікс /16 із двома старшими октетами для позначення адреси мережі, а інші два октети - як другий вузлів (понад 65 000 адрес вузлів у мережі).
- *Клас С (192.0.0.0 /24 - 223.255.255.0 /24)* – Розроблений для підтримки невеликих мереж з максимальною кількістю вузлів - 254. Клас С використовував фіксований префікс /24 із трьома першими октетами для позначення адреси мережі, а останній октет - як другий вузлів (тільки 254 адреси вузлів у мережі).

Також є блок групової розсилки (multicast) класу D (від 224.0.0.0 до 239.0.0.0) і блок експериментальних адрес класу E (від 240.0.0.0 до 255.0.0.0).

У той час при обмеженій кількості комп'ютерів, що використовувались в мережі Інтернет, класова адресація була ефективним способом розподілу

адрес. Мережі класів А і В мають дуже велику кількість адрес вузлів, а класу С – дуже малу. На мережі класу А припадало 50% мереж IPv4. Це призвело до того, що більшість доступних адрес IPv4 не використовується.

У середині 1990-х років, із впровадженням Всесвітнього павутиння (WWW), класова адресація стала застарілою для ефективного розподілу обмеженого адресного простору IPv4. Класова адресація була замінена більш новою і актуальною безкласовою системою адресації, яка використовується сьогодні. Безкласова адресація не використовує правила класів (А, В, С). Публічні мережні адреси IPv4 (мережні адреси та маски підмережі) виділяють виходячи з кількості адрес, які можуть бути виправдані.

Через виснаження публічного адресного простору IPv4, якомога краще використання доступних адрес вузлів є головною проблемою при створенні підмереж IPv4.

Використання більшої довжини адреси IPv6 дозволяє набагато простіше планувати та розподіляти адреси, ніж це дозволяє IPv4. Збереження IPv6-адрес не є проблемою. Це одна з вагомих причин для переходу на IPv6.

У традиційному розподілі на підмережі кожній підмережі виділяється однакова кількість адрес. Якщо всі підмережі мають однакові вимоги до кількості вузлів, або якщо збереження IPv4-адресного простору не є проблемою, ці блоки адрес фіксованого розміру будуть ефективними. Зазвичай із публічними адресами IPv4 це не так.

Маска підмережі змінної довжини (VLSM)

Через виснаження публічного адресного простору IPv4, якомога краще використання доступних адрес вузлів є головною проблемою при створенні підмереж IPv4.

Примітка: Використання більшої довжини адреси IPv6 дозволяє набагато простіше планувати та розподіляти адреси, ніж це дозволяє IPv4. Збереження IPv6-адрес не є проблемою. Це одна з вагомих причин для переходу на IPv6.

У традиційному розподілі на підмережі кожній підмережі виділяється однакова кількість адрес. Якщо всі підмережі мають однакові вимоги до кількості вузлів, або якщо збереження IPv4-адресного простору не є проблемою, ці блоки адрес фіксованого розміру будуть ефективними. Зазвичай із публічними адресами IPv4 це не так.

Маска підмережі змінної довжини (VLSM) була розроблена, щоб уникнути недоцільного витрачання адрес при розподілі мережі на підмережі.

При традиційній схемі розподілу на підмережі, створюються підмережі однакового розміру. Кожна підмережа в традиційній схемі використовує одну і ту ж маску підмережі. VLSM дозволяє розподілити мережний простір на нерівні частини. З VLSM маска підмережі буде змінюватися в залежності від того, скільки бітів було запозичено для конкретної підмережі, таким чином при використанні VLSM буде «змінна» частина маски. VLSM – це розподіл на підмережі меншого розміру.

5.7. Механізм перетворення мережевих адрес (NAT)

Кількість публічних IPv4-адрес є недостатньою, щоб призначити унікальну адресу кожному пристрою, з'єднаному з Інтернетом. Мережі зазвичай реалізуються за допомогою приватних адрес IPv4, як це визначено в RFC 1918.

Ці приватні адреси використовуються в організації або об'єкті з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці адреси не визначають конкретну компанію чи організацію, приватні IPv4-адреси не можна використовувати для маршрутизації через Інтернет. Щоб дозволити пристрою з приватною IPv4-адресою отримувати доступ до пристроїв та ресурсів поза межами локальної мережі, приватну адресу потрібно транслювати в публічну.

NAT забезпечує перетворення приватних адрес в публічні (рис. 5.3). Це дозволяє пристрою з приватною IPv4-адресою отримувати доступ до ресурсів за межами своєї приватної мережі, таких, що знаходяться в Інтернеті. NAT, у поєднанні з приватними IPv4-адресами, був основним методом збереження публічних IPv4-адрес. Одну приватну IPv4-адресу можуть використовувати сотні, навіть тисячі пристроїв, кожен з яких має унікальну приватну IPv4-адресу.

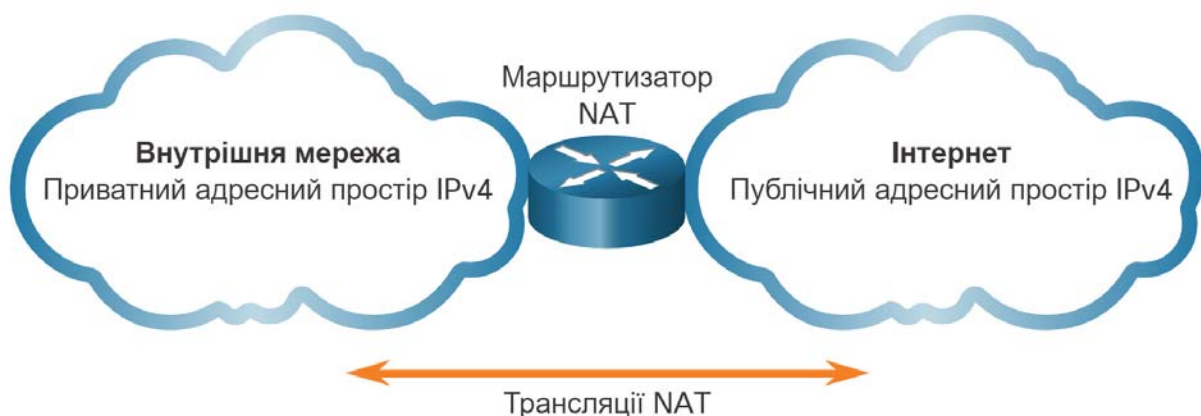


Рис. 5.3. Перетворення приватних адрес в публічні

NAT має багато застосувань, але основним його використанням є збереження публічних IPv4-адрес. Це досягається за рахунок того, що для внутрішньої взаємодії в мережах використовуються приватні IPv4-адреси, а перетворення в публічну адресу відбувається лише за потреби. Додаткова перевага NAT – підвищення ступеня конфіденційності і безпеки мережі – пояснюється тим, що даний механізм приховує внутрішні IPv4-адреси від зовнішніх мереж.

Маршрутизатори з підтримкою NAT можуть бути налаштовані з однієї або більшою кількістю дійсних публічних IPv4-адрес. Ці публічні адреси відомі як NAT-пул. Коли внутрішній пристрій надсилає трафік за межі мережі, маршрутизатор з підтримкою NAT перетворює внутрішню IPv4-адресу пристрою на публічну з NAT-пулу. Для зовнішніх пристроїв весь трафік, який входить до мережі та виходить з неї, має публічну IPv4-адресу із наданого пулу адрес.

Маршрутизатор NAT зазвичай працює на межі тупикової мережі. Тупикова мережа – це мережа, яка має одне з'єднання з сусідньою мережею, і, як наслідок, це один шлях з та до мережі. У прикладі на рисунку 5.4, R2 – граничний маршрутизатор. З точки зору інтернет-провайдера (ISP) R2 утворює тупикову мережу.

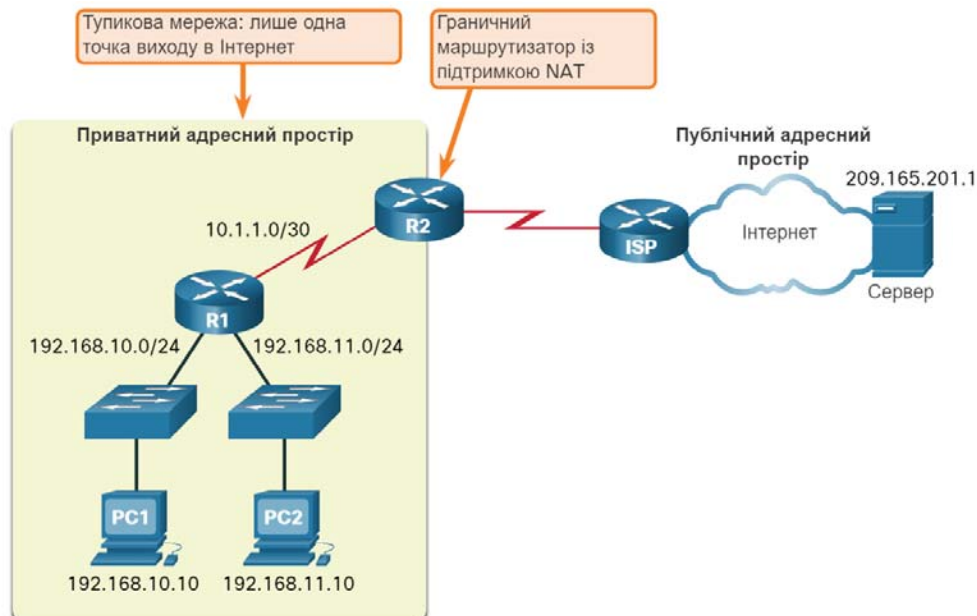


Рис. 5.4. Приклад мережі з NAT

Коли пристрою у тупиковій мережі потрібне під'єднання до пристрою поза власною мережею, пакет пересилається граничному маршрутизатору. Граничний маршрутизатор виконує NAT, транслюючи внутрішню приватну адресу пристрою в публічну, зовнішню, яка маршрутизується.

У термінології NAT під «внутрішньою мережею» мається на увазі набір мереж, чиї адреси будуть транслюватися. Термін «зовнішня мережа» відноситься до всіх інших мереж.

При використанні NAT адреси IPv4 мають різні позначення залежно від того, де вони знаходяться: в приватній або публічній мережі (Інтернет), і чи є трафік вхідним або вихідним.

NAT надає 4 типи адрес:

- *Внутрішня локальна адреса*
- *Внутрішня глобальна адреса*
- *Зовнішня локальна адреса*
- *Зовнішня глобальна адреса*

При визначенні використовуваного типу адреси важливо пам'ятати, що термінологія NAT завжди застосовується з точки зору пристрою, адреса якого буде транслюватися:

- *Внутрішня адреса* – адреса пристрою, яка транслюватиметься NAT.
- *Зовнішня адреса* – адреса пристрою призначення.

У рамках NAT щодо адрес також використовується поняття локальності або глобальності:

- *Локальна адреса* – це будь-яка адреса, що з'являється у внутрішній частині мережі.
- *Глобальна адреса* – це будь-яка адреса, що з'являється у зовнішній частині мережі.

Терміни «внутрішній» і «зовнішній» використовуються в поєднанні з термінами «локальний» і «глобальний», коли мова йде про конкретні адреси. Маршрутизатор NAT (на рисунку R2) є точкою розмежування між внутрішньою і зовнішньою мережами. R2 налаштований з використанням пулу публічних адрес, що призначаються внутрішнім вузлам. Наступний опис кожного з типів адрес NAT показано у таблиці NAT та мережі на рисунку 5.5.

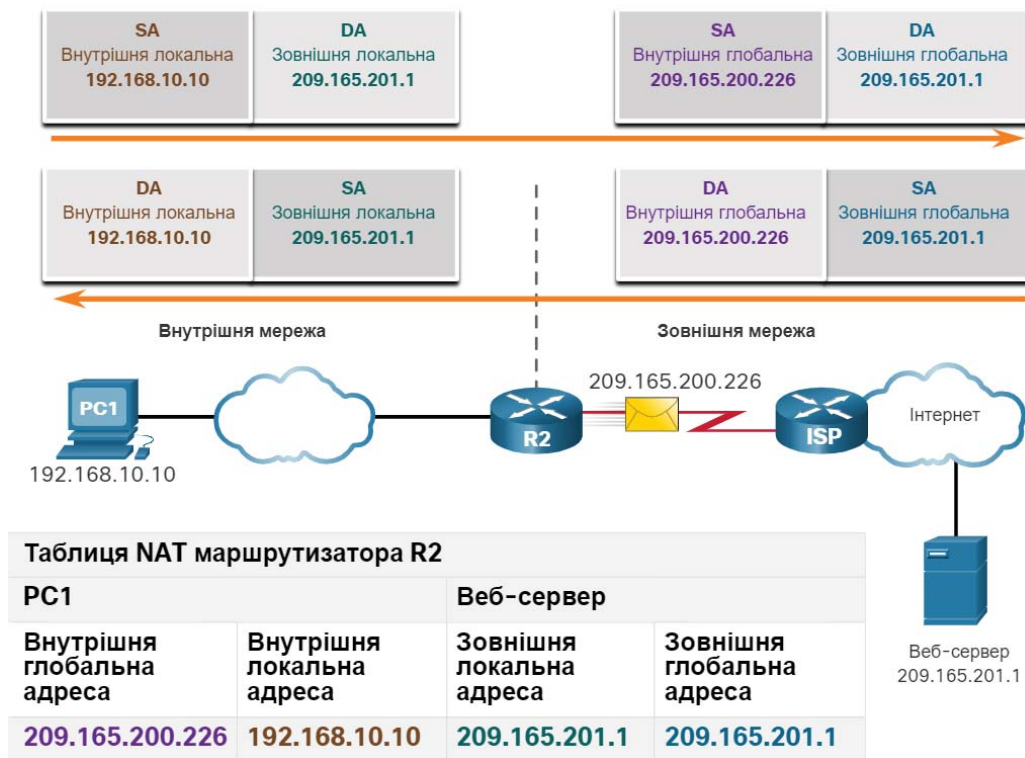


Рис.5.5. Типи адрес

5.7.1. Типи NAT

Статичний NAT

Статичний NAT (Static NAT) використовує зіставлення локальних і глобальних адрес за схемою «один до одного». Ці зіставлення налаштовуються системним адміністратором і залишаються незмінними.

Статичний NAT зручно використовувати для веб-серверів або пристроїв, які повинні мати статичну адресу, доступну в Інтернеті, наприклад, для веб-сервера компанії. Статичний NAT також підходить для пристроїв, до яких повинен мати доступ авторизований персонал, що працює поза межами офісу, але залишаються закритими для загального доступу в Інтернет.

Статичний NAT вимагає наявності достатньої кількості публічних адрес для усього числа одночасних сеансів користувача.

Динамічний NAT

Динамічний NAT (Dynamic NAT) використовує пул публічних адрес, які призначаються за правилом («першим прийшов – першим обслуговується»). При запиті внутрішнього пристрою на доступ до

зовнішньої мережі динамічний NAT призначає доступну публічну IPv4-адресу з пулу.

Трансляція адреси та номера порту (PAT)

Трансляція адреси та номера порту (PAT, Port Address Translation), також відома як NAT з перевантаженням, ставить у відповідність декілька приватних IPv4-адрес до однієї або декількох публічних IPv4-адрес. Так працює більшість домашніх маршрутизаторів. Інтернет-провайдер надає одну адресу маршрутизатору, завдяки чому кілька домашніх пристроїв мають можливість одночасно отримувати доступ до Інтернету. Це найпоширеніша форма NAT як для домашнього, так і для корпоративного використання.

За допомогою PAT безліч адрес можуть бути зіставлені з однією або декількома адресами, оскільки кожна приватна адреса також відстежується за номером порту. Коли пристрій починає TCP/IP сесію, він генерує значення порту джерела TCP або UDP або спеціально призначений ідентифікатор запиту для ICMP, щоб однозначно визначити сесію. При отриманні пакету від клієнта маршрутизатор NAT використовує номер порту джерела в пакеті для однозначного визначення NAT.

PAT гарантує, що пристрої будуть використовувати різний номер порту TCP для кожного сеансу взаємодії з сервером в Інтернеті. При отриманні відповіді з сервера номер порту джерела, який стає номером порту призначення при зворотному пересиланні, визначає, якому пристрою маршрутизатор надсилає пакети. Процес PAT також перевіряє запит на вхідні пакети, що підвищує ступінь захисту сесії.

Порівняння NAT і PAT

У таблиці наводиться зведена інформація про відмінності між NAT і PAT.

NAT	PAT
Зіставлення між внутрішніми локальними та внутрішніми глобальними адресами.	Одна внутрішня глобальна адреса може бути зіставлена з багатьма внутрішніми локальними адресами.

NAT	PAT
Використовує лише IPv4-адреси у процесі трансляції.	Використовує IPv4-адреси та номери портів джерела TCP або UDP у процесі трансляції.
Для кожного внутрішнього вузла, що отримує доступ до зовнішньої мережі, потрібна унікальна внутрішня глобальна адреса.	Єдина унікальна внутрішня глобальна адреса може бути розподілена між багатьма внутрішніми вузлами для доступу до зовнішньої мережі.

5.8. Адресація IPv6

Протокол IPv6 був розроблений як послідовник протоколу IPv4. Адреса IPv6 має великий 128-бітний адресний простір, що забезпечує 340 ундецильйонів (тобто 340, а потім 36 нулів) можливих адрес. Однак IPv6 – це більше, ніж просто велика кількість адрес.

Коли фахівці IETF почали розробку послідовника IPv4, вони використали цю можливість для виправлення обмежень IPv4 та внесення додаткових покращень. Одним із прикладів є протокол міжмережних керуючих повідомлень версії 6 (ICMPv6, Internet Control Message Protocol version 6) який включає в себе вирішення адрес та автоналаштування адрес, яких не було в ICMP для IPv4 (ICMPv4).

Сумісне використання протоколів IPv4 і IPv6

Точної дати для переходу на IPv6 поки що немає. Як IPv4, так і IPv6 будуть співіснувати найближчим часом, і перехід триватиме декілька років. Фахівці IETF створили різні протоколи та інструменти, які допомагають мережним адміністраторам поступово здійснити перехід своїх мереж на IPv6. Методи переходу можна розділити на три категорії:

Подвійний стек

Подвійний стек дозволяє IPv4 та IPv6 співіснувати в одному сегменті мережі. Пристрої подвійного стека одночасно працюють з протокольними стеками як IPv4, так і IPv6. Природне IPv6 - означає, що мережа клієнта IPv6 під'єднана до свого провайдера послуг Інтернету (ISP) і може отримувати доступ до вмісту, знайденого в Інтернеті через IPv6.

Тунелювання

Тунелювання — це метод передавання пакета IPv6 через мережу IPv4. Пакет IPv6 інкапсульований всередині пакета IPv4, аналогічно іншим типам даних.

Перетворення

Перетворення мережних адрес 64 (NAT64) дозволяє пристроям з підтримкою IPv6 взаємодіяти із пристроями з підтримкою IPv4 за допомогою методу перетворення, аналогічного NAT для IPv4. Пакет IPv6 перетворюється в пакет IPv4, а пакет IPv4 - у пакет IPv6.

5.8.1. Формати адрес IPv6

Адреси IPv6 мають довжину 128 бітів і записуються у вигляді рядка шістнадцяткових значень. Кожні чотири біти представлено однією шістнадцятковою цифрою; загалом 32 шістнадцяткових значень, як показано на рисунку. IPv6-адреси не чутливі до регістру і можуть бути записані як в нижньому регістрі, так і у верхньому.

Основний формат

Основний формат для запису IPv6-адреси – x: x: x: x: x: x: x: x, при цьому кожен x складається з чотирьох шістнадцяткових значень. Термін октет відноситься до восьми бітів IPv4-адреси. Для IPv6 гекстет (hextet) – неофіційний термін, який використовують для позначення сегмента з 16 бітів або чотирьох шістнадцяткових значень. Кожен x – це один гекстет, 16 бітів або чотири шістнадцяткові цифри.

Основний формат означає, що ви записуєте IPv6-адресу, використовуючи всі 32 шістнадцяткові цифри. Однак, це не самий досконалий спосіб подання адреси IPv6. Існує два правила, які допоможуть зменшити кількість цифр, необхідних для подання IPv6-адреси.

Правило 1 – Пропуск початкових нульових розрядів

Перше правило, яке допоможе скоротити запис адреси IPv6 – це пропуск усіх початкових нулів (0) у будь-якому гексеті. Ось чотири приклади способів пропуску початкових нулів:

- 01ab можна подати як 1ab
- 09f0 можна подати як 9f0
- 0a00 можна подати як a00
- 00ab можна подати як ab

Це правило застосовується лише до початкових 0, а НЕ до кінцевих 0, інакше адреса буде незрозумілою. Наприклад, текст «abc» може бути «0abc» або «abc0», але вони не подають одне і те ж значення.

Таблиця 5.3.

Пропуск початкових нулів

<i>Тип</i>	<i>Формат</i>
Основний формат	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Без початкових нулів	2001 : db8 : 0 : 1111 : 0 : 0 : 0 : 200
Основний формат	2001 : 0db8 : 0000 : 00a3 : ab00 : 0ab0 : 00ab : 1234
Без початкових нулів	2001 : db8 : 0 : a3 : ab00 : ab0 : ab : 1234

Правило 2 – Подвійна двокрапка

Друге правило, яке допомагає скоротити запис адрес IPv6, полягає в тому, що подвійні двокрапки (::) можуть замінити будь-який єдиний, суміжний рядок одного або декількох 16-бітних гексетів, що складаються з усіх нулів. Наприклад, 2001:db8:cafe:1:0:0:0:1 (початкові 0 не вказано) можна подати як 2001:db8:cafe:1::1. Подвійні двокрапки (::) використовуються замість трьох нульових гексетів, всі-0 (0:0:0).

Подвійні двокрапки (::) можуть використовуватися лише один раз у межах адреси, інакше в результаті може виникнути декілька адрес. Поєднання цього правила з способом пропуску початкових нулів допомагає значно скоротити запис адреси IPv6. Зазвичай це називається стисненим форматом.

Наведемо приклад неправильного використання подвійних двокрапок: 2001:db8::abcd::1234.

Подвійні двокрапки використовуються двічі в наведеному вище прикладі. Нижче наведено можливі розширення цієї адреси з неправильним стисненим форматом:

- 2001:db8::abcd:0000:0000:1234
- 2001:db8::abcd:0000:0000:0000:1234

- 2001:db8:0000:abcd::1234
- 2001:db8:0000:0000:abcd::1234

Якщо адреса містить більше одного суміжного рядка з усіма 0 гекстетами, то найкращою практикою є використання подвійних двокрапок (::) у найдовшому рядку. Якщо рядки рівні, перший рядок повинен використовувати подвійні двокрапки (::).

Таблиця 5.4.

Пропуск початкових 0 і всіх 0 сегментів

<i>Тип</i>	<i>Формат</i>
Основний	2001 : 0db8 : 0000 : 1111 : 0000 : 0000 : 0000 : 0200
Стислий/пробіли	2001 : db8 : 0 : 1111 : : 200
Стислий	2001:db8:0:1111::200
Основний	2001 : 0db8 : 0000 : 0000 : ab00 : 0000 : 0000 : 0000
Стислий/пробіли	2001 : db8 : 0 : 0 : ab00 ::
Стислий	2001:db8:0:0:ab00::

5.8.2. Типи адрес IPv6

Індивідуальна, групова, альтернативна адреси

Як і у IPv4, існують різні типи IPv6-адрес. По суті, існує три широкі категорії IPv6-адрес:

- *Індивідуальна (unicast)* – Індивідуальна адреса IPv6 однозначно ідентифікує інтерфейс на пристрої з підтримкою IPv6.
- *Групова (multicast)* – Групова адреса IPv6 використовується для надсилання одного пакета IPv6 на декілька адрес призначення.
- *Альтернативна (anycast)* – Альтернативна адреса IPv6 - це будь-яка індивідуальна адреса IPv6, яку можна призначати декільком пристроям. Пакет, надісланий на альтернативну адресу, перенаправляється до найближчого пристрою, який має цю адресу.

На відміну від IPv4, IPv6 не використовує широкомовної адреси. Однак, є групова адреса IPv6 для усіх вузлів, що дає аналогічний результат.

Довжина префікса IPv6

Нагадаємо, що префікс або мережну частину IPv4-адреси можна ідентифікувати за допомогою маски підмережі або довжини префікса (число після скісної риски). Наприклад, IPv4-адреса 192.168.1.10 з маскою підмережі в десятковому форматі розділеному крапками 255.255.255.0 еквівалентна запису 192.168.1.10/24.

У IPv4 – /24 називається префіксом. У IPv6 – це називається довжиною префікса. IPv6 не використовує запис маски в десятковому форматі розділеному крапками. Як і IPv4, довжина префікса представлена скісною рисою та використовується для позначення мережної частини адреси IPv6.

Довжина префікса може бути в діапазоні від 0 до 128. Рекомендована довжина префікса IPv6 для локальних мереж та більшості інших типів мереж – /64, як показано на рисунку.

На графіку показано IPv6-адресу, розділену на 64-бітний префікс і 64-бітний ідентифікатор інтерфейсу. 64-розрядний префікс – 2001:0db8:000a:0000. 64-розрядний ідентифікатор інтерфейсу – 0000:0000:0000:0000.

Строго рекомендовано використовувати 64-бітний ідентифікатор інтерфейсу для більшості мереж. Це відбувається тому, що для автоналаштування адреси без збереження стану (SLAAC) використовується 64 біти для ідентифікатора інтерфейсу. Це також полегшує створення підмереж та їх керування.



Префікс або мережна частина адреси має довжину 64 біти, залишаючи ще 64 біти для ідентифікатора інтерфейсу (вузлової частини) адреси.

Типи індивідуальних адрес IPv6

Індивідуальна адреса IPv6 однозначно ідентифікує інтерфейс на пристрої з підтримкою IPv6. Пакет, який надсилається на таку адресу, буде отримано інтерфейсом, призначеним для цієї адреси. Аналогічно до IPv4, IPv6-адреса джерела повинна бути індивідуальною адресою. IPv6-адреса призначення може бути як індивідуальною, так і груповою. На рисунку показано різні типи індивідуальних адрес IPv6.

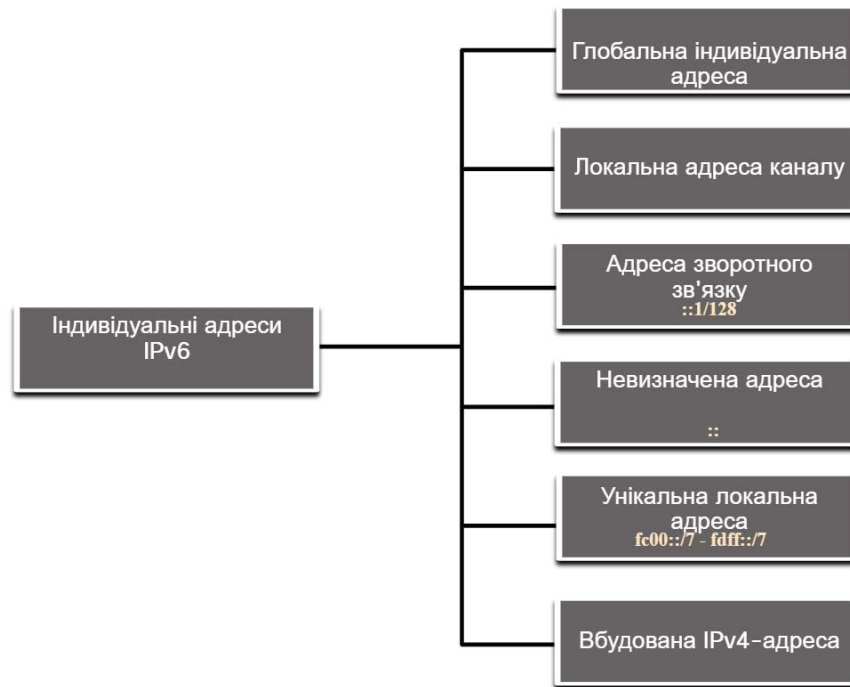


Рис. 5.6. Типи індивідуальних адрес IPv6

На відміну від пристроїв IPv4, які мають тільки одну адресу, IPv6-адреси зазвичай мають дві індивідуальні (unicast) адреси:

- *Глобальну індивідуальну адресу (GUA)* – аналогічну публічній адресі IPv4. Це глобально унікальні в усьому світі адреси, що маршрутизуються в Інтернеті. Глобальні індивідуальні адреси можуть налаштовуватися статично або призначатися динамічно.

- *Локальну адресу каналу (LLA)* – потрібну для кожного пристрою з підтримкою IPv6. Локальні адреси каналу використовуються для зв'язку з іншими пристроями в одному локальному каналі. З IPv6 термін "канал" відноситься до підмережі. Локальні адреси обмежуються одним каналом. Їх унікальність повинна бути підтверджена тільки в межах цього каналу, оскільки вони не підлягають маршрутизації поза межами каналу. Іншими словами, маршрутизатори не зможуть перенаправляти пакети, маючи локальну адресу каналу джерела або адресу призначення.

Глобальні індивідуальні адреси IPv6

Глобальні індивідуальні адреси IPv6 глобально унікальні та доступні для маршрутизації в Інтернеті IPv6. Ці адреси аналогічні публічним адресам IPv4. Інтернет-комітет призначення імен і номерів (ICANN, Internet Committee for Assigned Names and Numbers), оператор для IANA, виділяє блоки адрес IPv6 на п'ять RIR. В даний час призначаються тільки глобальні індивідуальні адреси з першими трьома бітами 001 або 2000::/3, як показано на рисунку.

На рисунку показано діапазон значень для першого гекстету, де перша шістнадцяткова цифра для наявних на даний момент GUA починається з 2 або 3. Це лише 1/8 частина всього доступного адресного простору IPv6, за винятком лише дуже незначної частини для інших типів індивідуальних та групових адрес.

Адреса IPv6 з префіксом глобальної маршрутизації /48 і префіксом /64



Глобальна індивідуальна адреса має три частини:

- Префікс глобальної маршрутизації
- Ідентифікатор підмережі
- Ідентифікатор інтерфейсу

Структура глобальної індивідуальної адреси IPv6

Префікс глобальної маршрутизації

Префікс глобальної маршрутизації – це префіксна або мережна частина адреси, яка призначається постачальником, наприклад, інтернет-провайдером, клієнту чи мережі. Наприклад, звичайним є, що постачальники послуг Інтернету (ISP) призначають своїм клієнтам префікс маршрутизації /48. Префікс глобальної маршрутизації залежить від політики постачальника послуг Інтернету (ISP).

На попередньому рисунку показано GUA, що використовує префікс глобальної маршрутизації /48. Префікси /48 – найбільш поширені префікси

глобальної маршрутизації, які призначаються і саме вони будуть використовуватися в більшості прикладів в рамках даного курсу.

Наприклад, IPv6-адреса 2001:db8:acad::/48 має префікс глобальної маршрутизації, який вказує, що перші 48 бітів (3 гексети) (2001:db8:acad) - це префіксна або мережна частина адреси, яка відома постачальнику послуг Інтернету. Подвійні двокрапки (::) перед довжиною префікса /48 означають, що інша частина адреси складається з усіх 0. Розмір префікса глобальної маршрутизації визначає розмір ідентифікатора підмережі.

Ідентифікатор підмережі

Поле Ідентифікатор підмережі (Subnet ID) – це область між префіксом глобальної маршрутизації та ідентифікатором інтерфейсу (Interface ID). На відміну від IPv4, де для створення підмереж потрібно запозичати біти з вузлової частини, протокол IPv6 був розроблений з урахуванням підмереж. Ідентифікатор підмережі використовується організаціями для позначення підмереж в межах своєї мережі. Чим вище значення ідентифікатора підмережі, тим більше існує підмереж.

Багато організацій отримують префікс глобальної маршрутизації /32. Використовуючи рекомендований префікс /64 для створення 64-розрядного ідентифікатора інтерфейсу, залишається 32-бітний ідентифікатор підмережі. Це означає, що організація з глобальним префіксом маршрутизації /32 та 32-розрядним ідентифікатором підмережі матиме 4,3 мільярда підмереж, кожна з яких включатиме 18 квінтильйонів пристроїв у підмережі. Це стільки підмереж, скільки є публічних IPv4-адрес!

Адреса IPv6 на попередньому рисунку має префікс глобальної маршрутизації /48, який є загальним для багатьох корпоративних мереж. Це дозволяє полегшити вивчення різних частин адреси. Використовуючи загальну довжину префікса /64, перші чотири гексети призначені для мережної частини адреси, а четвертий гекстет вказує на ідентифікатор підмережі. Решта чотири гексети призначені для ідентифікатора інтерфейсу.

Ідентифікатор інтерфейсу

Ідентифікатор інтерфейсу IPv6 еквівалентний вузловій частині адреси IPv4. Термін Ідентифікатор інтерфейсу використовується в тому випадку, коли один вузол може мати кілька інтерфейсів, кожен з яких має одну або більше IPv6-адрес. Наполегливо рекомендується в більшості випадків

використовувати префікс підмережі /64, що створює 64-бітний ідентифікатор інтерфейсу. 64-бітний ідентифікатор інтерфейсу дозволяє використовувати 18 квінтильйонів пристроїв або вузлів у підмережі.

Підмережа або префікс /64 (префікс глобальної маршрутизації + ідентифікатор підмережі) залишає 64 біти для ідентифікатора інтерфейсу. Рекомендується, щоб пристрої з підтримкою SLAAC створювали власний 64-бітний ідентифікатор інтерфейсу. Це також робить розроблення плану адресації IPv6 простим та ефективним.

На відміну від IPv4, при використанні протоколу IPv6 пристрою можна призначати адресу вузла, що складається з усіх 0 або з усіх 1. Адресу, яка містить всі 1 можна використовувати, оскільки широкомовні адреси не використовуються в IPv6. Також можна використовувати адресу, яка містить всі 0 але вона зарезервована як альтернативна (anycast) адреса підмережі маршрутизатора і повинна призначатися тільки маршрутизаторам.

Локальна IPv6-адреса каналу

Локальна IPv6-адреса каналу дозволяє пристрою взаємодіяти з іншими пристроями з підтримкою IPv6, що знаходяться в одному і тому ж каналі (підмережі) і тільки в ньому. Пакети з локальною адресою каналу джерела або призначення не можуть бути перенаправлені поза межі каналу, в якому створюється пакет.

Глобальної індивідуальної адреси не обов'язково. Однак кожному IPv6-сумісному мережному інтерфейсу необхідно мати локальну адресу каналу (LLA).

Якщо локальну адресу каналу не налаштовано статично на інтерфейсі, пристрій автоматично створює її самостійно, не звертаючись до сервера DHCP. Вузли з підтримкою IPv6 створюють локальну IPv6-адресу каналу, навіть в тому випадку, якщо пристрою не було призначено глобальну індивідуальну адресу IPv6. Це дозволяє пристроям з підтримкою IPv6 взаємодіяти між собою в одній підмережі, зокрема зі шлюзом за замовчуванням (маршрутизатором).

Локальні IPv6-адреси каналу знаходяться в діапазоні fe80::/10. Довжина префікса /10 вказує, що перші 10 бітів - 1111 1110 10xx xxxx. Діапазон значень першого гекстета: від 1111 1110 1000 0000 (fe80) до 1111 1110 1011 1111 (febf).

Існує два способи, за допомогою яких пристрій може отримувати локальну адресу каналу (LLA):

- *Статично* - це означає, що пристрій було налаштовано вручну.
- *Динамічно* – це означає, що пристрій створює власний ідентифікатор інтерфейсу, використовуючи випадково згенеровані значення або використовуючи розширений унікальний ідентифікатор (EUI, Extended Unique Identifier), який використовує MAC-адресу клієнта разом з додатковими бітами.

Групові адреси IPv6

Групові адреси IPv6 аналогічні груповим (багатоадресним) адресам IPv4. Групова адреса (multicast) використовується для надсилання одного пакета одній або декільком адресам призначення (групі групової розсилки). Групові адреси IPv6 мають префікс ff00::/8.

Групові адреси можуть бути тільки адресами призначення, а не адресами джерела.

Групові адреси IPv6 поділяються на два типи:

- Відомі групові адреси
- Групові адреси запитуваного вузла

Відомі групові адреси

Призначено відомі адреси групової розсилки IPv6. Призначені групові адреси - це зарезервовані групові адреси для попередньо визначеної групи пристроїв. Призначена групова адреса - це одна адреса, яка використовується для доступу до групи пристроїв, що працюють із одним протоколом або службою. Призначені групові адреси використовуються у контексті з конкретними протоколами, наприклад DHCPv6.

Є дві поширені групи призначених групових адрес IPv6:

- *ff02::1 Групова розсилка для усіх вузлів* – це групова розсилка, до якої під'єднуються усі пристрої з підтримкою IPv6. Пакет, який надійшов у цю групу, приймається і обробляється усіма інтерфейсами IPv6 в каналі або мережі. Ця група адрес працює так само, як широкомовна адреса в IPv4. На рисунку наведено приклад комунікації за допомогою групових адрес для усіх вузлів. Маршрутизатор IPv6 надсилає повідомлення RA ICMPv6 для усіх вузлів групової розсилки.

- *ff02::2 Групова розсилка для усіх маршрутизаторів* – це групова розсилка, до якої під'єднуються усі маршрутизатори IPv6. Маршрутизатор

стає учасником цієї групи, якщо його увімкнено як маршрутизатор IPv6 командою *ipv6 unicast routing* режиму глобальної конфігурації. Пакет, який надійшов у цю групу, приймається і обробляється всіма маршрутизаторами IPv6 в каналі або мережі.

Групова IPv6-адреса запитуваного вузла

Групова адреса запитуваного вузла подібна до адреси групової розсилки для усіх вузлів. Перевага групової адреса запитуваного вузла полягає в тому, що вона зіставляється з особливою груповою адресою Ethernet. Це дозволяє мережній платі Ethernet фільтрувати кадр, аналізуючи MAC-адресу призначення, не надсилаючи його до процесу IPv6, щоб переконатися, що пристрій дійсно є вузлом призначення пакету IPv6.

Контрольні запитання

1. Що таке мережний рівень в моделі OSI і яку функцію він виконує?
2. Які основні протоколи мережного рівня використовуються в інтернеті?
3. Які чотири основні операції виконує мережний рівень для забезпечення наскрізного зв'язку через межі мереж?
4. Що таке інкапсуляція на мережному рівні, і які дані додаються до пакету під час цього процесу?
5. Яку роль відіграє маршрутизатор у мережному рівні, і що таке маршрутизація?
6. Що таке деінкапсуляція на мережному рівні і коли вона відбувається?
7. Які основні характеристики має протокол IP (IPv4)?
8. Чому протокол IP називається ненадійним і не гарантує доставку пакетів?
9. Які переваги має IPv6 порівняно з IPv4?
10. Які основні різниці між заголовками пакетів IPv4 і IPv6?
11. Що таке IPv4-адрес, і які частини входять до його складу?
12. Які біти в мережній частині адреси IPv4 і для чого вони використовуються?
13. Які біти вузлової частини адреси IPv4 і для чого вони використовуються?
14. Як визначити, чи два вузли належать до однієї і тієї ж мережі IPv4?

15. Що таке маска підмережі IPv4, і як вона використовується?
16. Які типи IP-адрес використовуються у межах кожної мережі?
17. Що таке ширококомовна адреса IPv4 і в яких ситуаціях вона використовується?
18. Які два типи ширококомовної розсилки існують, і яка їх різниця?
19. Яким чином групова розсилка (Multicast) відрізняється від ширококомовної розсилки (Broadcast) у IPv4?
20. Що таке публічні та приватні адреси IPv4, і в яких ситуаціях вони використовуються?
21. Як відбувається трансляція мережних адрес (NAT) у IPv4 і для чого вона потрібна?
22. Які адреси відносяться до адрес спеціального призначення IPv4, і як вони використовуються?
23. Як визначається клас IPv4-адреси, і які класи існують?
24. Що таке VLSM, і як вона відрізняється від традиційного розподілу на підмережі?
25. Яким чином IPv6 відрізняється від IPv4 за розміром адресного простору?
26. Які переваги має протокол ICMPv6 порівняно з ICMP для IPv4?
27. Якими методами можна здійснювати перехід на IPv6 у мережі?
28. Що означає термін "подвійний стек" в контексті IPv6?
29. Як працює метод тунелювання для передачі пакетів IPv6 через мережу IPv4?
30. Яким чином працює перетворення мережних адрес (NAT64) для взаємодії пристроїв з підтримкою IPv6 та IPv4?
31. Як записуються адреси IPv6 в основному форматі?
32. Які правила допомагають зменшити кількість цифр, необхідних для подання IPv6-адреси?

РОЗДІЛ 6. ОГЛЯД ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ

6.1. Загальні характеристики

Основна функція маршрутизатора – перемістити IP-пакет з однієї мережі до іншої. Маршрутизатор дізнається про неприєднані мережі за допомогою налаштування статичних маршрутів або через протоколи динамічної IP-маршрутизації.

Протокол динамічної маршрутизації дозволяє маршрутизаторам автоматично отримувати інформацію про віддалені мережі, включаючи маршрут за замовчуванням, з інших маршрутизаторів. Маршрутизатори, які використовують протоколи динамічної маршрутизації, автоматично обмінюються інформацією про маршрутизацію з іншими маршрутизаторами і враховують будь-які зміни топології без залучення адміністратора мережі. При зміні топології мережі маршрутизатори поширюють цю інформацію за допомогою протоколу динамічної маршрутизації і автоматично оновлюють свої таблиці маршрутизації.

Протоколи динамічної IP-маршрутизації передають інформацію про топологію мережі між маршрутизаторами та пересилають оновлення автоматично, коли відбуваються зміни топології в мережі. Вимоги до мережі чи апаратні обмеження можуть обмежити IP-маршрутизацію статичними маршрутами, які не дуже добре пристосовуються до змін топології.

При використанні протоколів динамічної маршрутизації маршрутизатори вибирають найкращий шлях без петель, яким пересилати пакет на IP-адресу призначення.

Мережа взаємопов'язаних маршрутизаторів та пов'язаних систем, які адмініструються в рамках спільної мережі, називається *автономною системою* (AS) або доменом маршрутизації. Інтернет складається з тисяч автономних систем, що охоплюють всю земну кулю.

Загальні протоколи динамічної маршрутизації, які використовуються сьогодні на більшості платформ маршрутизації:

- Протокол маршрутної інформації версії 2 (RIPv2).
- Розширена маршрутизація через внутрішній шлюз (EIGRP).
- Протокол динамічної маршрутизації, що базується на технології відстеження стану каналу (OSPF).
- Протокол маршрутизації проміжних систем (IS-IS).
- Протокол прикордонного шлюзу (BGP).

За винятком BGP, протоколи в цьому списку розроблені та оптимізовані для маршрутизації всередині автономної системи та відомі як протоколи внутрішніх шлюзів (IGP).

Протоколи зовнішнього шлюзу (EGP) маршрутизують між автономними системами. BGP – це протокол EGP, але він також може використовуватися в автономній системі. Якщо BGP обмінюється маршрутами в автономній системі, це називається внутрішнім сеансом BGP (iBGP). Якщо він обмінюється маршрутами між різними автономними системами, він відомий як зовнішній BGP (eBGP).

На рис. 6.1 показано, як можуть працювати один або кілька протоколів IGP, а також iBGP всередині автономної системи та як eBGP з'єднують різні автономні системи разом.

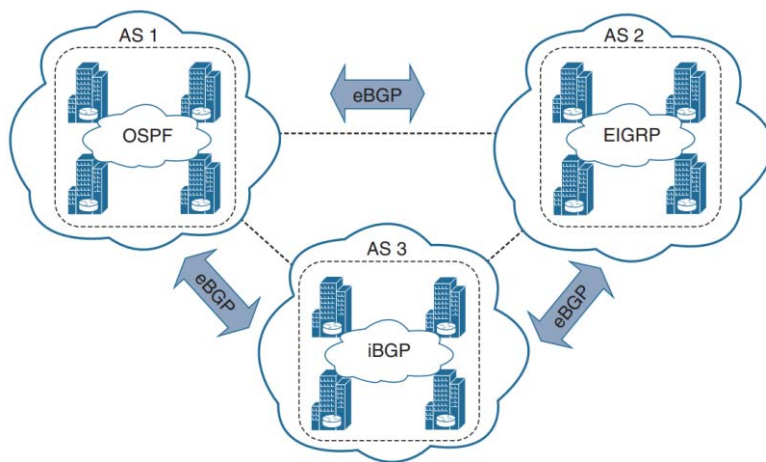


Рис. 6.1 Автономні системи BGP та їх взаємодія.

6.2. Алгоритм дистанційно-векторних протоколів

Протоколи дистанційно-векторної маршрутизації, такі як RIP, оголошують маршрути як вектори, де відстань метрика (або вартість), розраховується як кількість переходів, а вектор – це IP-адреса маршрутизатора наступного переходу, яка використовується для досягнення мережі призначення:

- Дистанція: це показник маршруту до мережі призначення.
- Вектор: це інтерфейс або напрямок мережі призначення.

Коли маршрутизатор отримує маршрутну інформацію від сусіда, він зберігає їх у локальному файлі маршрутизації. База даних у міру її наповнення та дистанційно-векторний алгоритм (розробка Беллмана-Форда та Форда-Фалкерсона) використовуються для визначення того, які шляхи є

найкращими шляхами без петель до кожної досяжної мережі призначення. Коли найкращі шляхи визначені, вони записуються в таблицю маршрутизації та оголошуються кожному сусідньому маршрутизатору.

Маршрутизатори, які використовують дистанційно-векторні протоколи, повідомляють інформацію про маршрутизацію своїм сусідам зі свого погляду, модифіковані порівняно з вихідним отриманим маршрутом. Тому дистанційно-векторний протокол немає повної топології всієї мережі; натомість його база даних відображає лише те, що знає сусідній маршрутизатор. Перевага цих протоколів полягає в тому, що вони вимагають менше ресурсів процесора та пам'яті та можуть працювати на недорогих маршрутизаторах.

Рисунок 6.2 показує, як маршрутизатор, що використовує дистанційно-векторний протокол, переглядає мережу і напрямок, в якому повинен рухатися пакет з R3, щоб досягти підмережі 192.168.1.0/24.

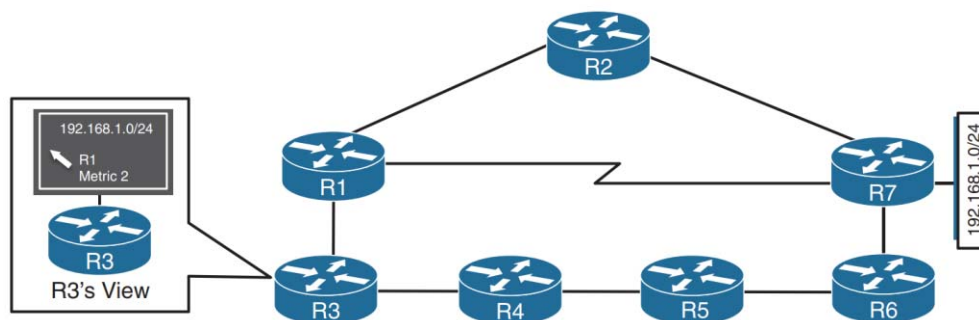


Рис. 6.2. Приклад мережі за дистанційно-векторним протоколом

Дистанційно-векторний протокол вибирає шляхи виключно на основі відстані. Не враховується швидкість з'єднання чи інші фактори. На рисунку 6.2 канал між R1 і R7 є послідовним каналом з пропускнуою здатністю всього 64 Кбіт/с, а всі інші канали являють собою канали Ethernet зі швидкістю 1 Гбіт/с. RIP не приймає це до уваги і перенаправляє трафік у цьому напрямку, що призведе до втрати пакетів, коли цей напрямок перевантажено.

6.3. Удосконалені алгоритми вектора відстані

Алгоритм дифузного оновлення (DUAL) – це вдосконалений алгоритм вектора відстані. Протокол EIGRP використовує цей алгоритм для розрахунку найкоротшого шляху до призначення в мережі. EIGRP анонсує мережеву інформацію своїм сусідам, як це роблять дистанційно-векторні протоколи, але має деякі поліпшення. Нижче наведено деякі з них:

- Забезпечує швидку конвергенцію під час зміни топології мережі.
- Надсилає оновлення лише при зміні мережі. Він відправляє повну таблицю маршрутизації, як це роблять дистанційно-векторні протоколи.
- Використовує привітання та формує сусідські відносини так само, як це роблять протоколи стану каналу.
- Використовує смугу пропускання, затримку, надійність, навантаження та максимальний розмір блоку передачі (MTU) замість кількості переходів для розрахунку метрики.
- Є можливість балансування навантаження трафіку по колії з рівною або нерівною вартістю.

EIGRP – це пропрієтарний протокол Cisco. Його іноді називають протоколом гібридної маршрутизації, оскільки має характеристики як дистанційно-векторний протокол, і протокол стану каналу. EIGRP покладається більш досконалі показники, відмінні кількості переходів (наприклад, пропускна спроможність) до розрахунку кращого шляху. За замовчуванням EIGRP використовує загальну затримку колії та мінімальну пропускну здатність для розрахунку метрики маршруту. Ця інформація анонсується на всі напрямки, як і дистанційно-векторного протоколу. Кожен маршрутизатор може розрахувати найкращий шлях на основі інформації, яка надходить від його безпосередніх сусідів. На рисунку 3 показано попередню топологію, але тепер у ній включені розрахунки метрик EIGRP. R3 повинен переслати пакети до мережі 192.168.1.0/24. Якщо домен маршрутизації використовує протокол дистанційно-векторної маршрутизації, він використовуватиме шлях R3→R1→R7, який знаходиться всього у двох стрибках, а не шлях R3→R1→R2→R7, який знаходиться на відстані трьох стрибків. Але шлях R3→R1→R7 не може підтримувати трафік вище 64 кбіт/с. В той час, як R3→R1→R2→R7 шлях довший, він забезпечує більшу пропускну здатність і не має такої великої затримки і є шляхом, вибраним EIGRP.

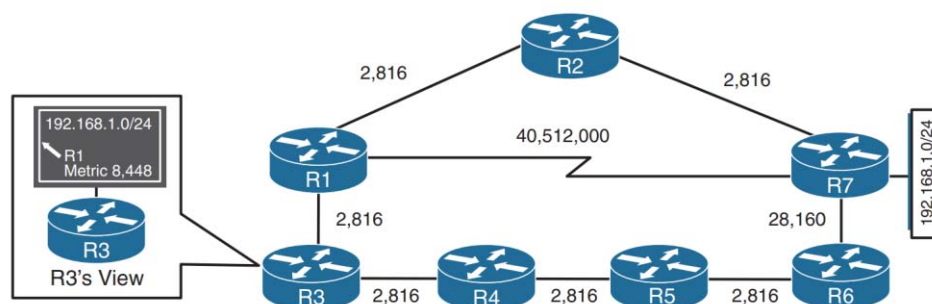


Рисунок 6.3. Дистанційно-векторний протокол порівняно з EIGRP

6.4. Протоколи стану каналу

Протокол OSPF (Open Shortest Path First) – це внутрішній маршрутизаційний протокол, який використовується в комп'ютерних мережах для визначення оптимальних маршрутів між маршрутизаторами. OSPF є одним із найпоширеніших протоколів маршрутизації в мережах, які використовуються внутрішніми маршрутизаторами.

OSPF є відкритим стандартом, що означає, що його специфікації доступні для публічного огляду і використання. Це сприяє інтегруєбельності між різними виробниками мережевого обладнання.

Протокол OSPF версії 2 (OSPFv2): визначений у RFC 2328 та підтримує IPv4.

Протокол OSPF версії 3 (OSPFv3): визначений у RFC 5340 для підтримки IPv6

Внутрішній протокол: OSPF призначений для внутрішньої маршрутизації в межах однієї адміністративної домену, так званої "AS" (Autonomous System). Він не використовується для маршрутизації між різними AS.

Link-State протокол: OSPF є протоколом, який використовує інформацію про стан зв'язків (link-state) для прийняття рішень щодо маршрутизації. Кожен маршрутизатор OSPF веде базу даних зв'язків, яка описує всі зв'язки в мережі та їх стани.

Основний принцип роботи OSPF полягає в обміні LSAs (Link-State Advertisements) між сусідніми маршрутизаторами для синхронізації їх баз даних зв'язків. Після синхронізації маршрутизатори визначають оптимальні маршрути до всіх мереж у мережі.

Оголошення про стан каналу (LSA) і включає відомості про маршрутизатори, канали та сегменти мережі. Отримані LSA зберігаються в локальній базі даних, яка називається базою даних стану каналу (LSDB), і вони розсилаються по домену маршрутизації OSPF так само, як рекламний роутер рекламував їх.

Усі маршрутизатори OSPF підтримують синхронізовану ідентичну копію LSDB для тієї ж області. LSDB зберігає топологію мережі, по суті надаючи маршрутизатору повну карту мережі. Усі маршрутизатори OSPF спочатку використовують найкоротший шлях Дейкстри (SPF). OSPF динамічно виявляє зміну топології в мережі та робить обчислення шляхів без петель за короткий час.

OSPF використовує метрику вартості для визначення найкращого шляху до місця призначення. Вартість посилення обернено пропорційна її пропускній спроможності. Канали з більш низькою пропускною здатністю мають більш високі витрати, тому OSPF віддає перевагу дорогам з більш високою пропускною здатністю. OSPF швидко реагує на зміни в мережі, оскільки маршрутизатори обмінюються оновленнями стану каналу при змінах мережі, таких як збої або додавання каналів. Це забезпечує швидшу конвергенцію та скорочує час, необхідний мережі для стабілізації після зміни топології.

OSPF дозволяє використовувати багатоколіїну маршрутизацію з рівною вартістю (ECMP), коли кілька шляхів з однаковою вартістю до пункту призначення можуть використовуватися одночасно, розподіляючи навантаження трафіку цими шляхами.

OSPF надає механізми аутентифікації для захисту обміну інформацією між маршрутизаторами з підтримкою OSPF.

Мережі OSPF зазвичай організовуються в області (зони) для покращення масштабованості та зменшення обсягу інформації про маршрутизацію, яку має підтримувати кожен маршрутизатор. Маршрутизатори всередині області мають докладніші відомості про топологію області, у той час як у них менше інформації про інші області.

Внутрішній маршрутизатор області: маршрутизатор, усі інтерфейси якого знаходяться в області OSPF.

Прикордонний маршрутизатор області (ABR): Маршрутизатор, який з'єднує декілька областей OSPF та бере участь у обміні маршрутною інформацією між ними.

Прикордонний маршрутизатор автономної системи (ASBR): маршрутизатор, який з'єднує домен OSPF з маршрутизаторами поза автономною системою OSPF.

Магістральний маршрутизатор: Маршрутизатор, який знаходиться у магістральній області OSPF (область 0) та підключається до інших областей OSPF. OSPF широко використовується у великомасштабних корпоративних мережах та середовищах постачальників послуг. Ефективне використання мережевих ресурсів та швидка збіжність роблять його важливим протоколом маршрутизації для забезпечення надійного та масштабованого зв'язку в автономній системі.

Кожна область OSPF надає набір підключених мереж та хостів, які згруповані разом. OSPF використовує дворівневу ієрархічну архітектуру, де

область 0 є спеціальна область, відома як магістраль, до якої повинні підключатися всі інші області. Іншими словами, область 0 забезпечує транзитне з'єднання між немагістральними областями. Немагістральні області оголошують маршрути до магістралі, а магістраль потім оголошує маршрути до інших немагістральних областей.

На рис. 6.4 показано оголошення маршруту до інших областей. Маршрути Зони 12 рекламуються для зони 0, а потім у зону 34. Маршрути із зони 34 оголошуються в зону 0, а потім зону 12.

Маршрути області 0 оголошуються в інші області OSPF.

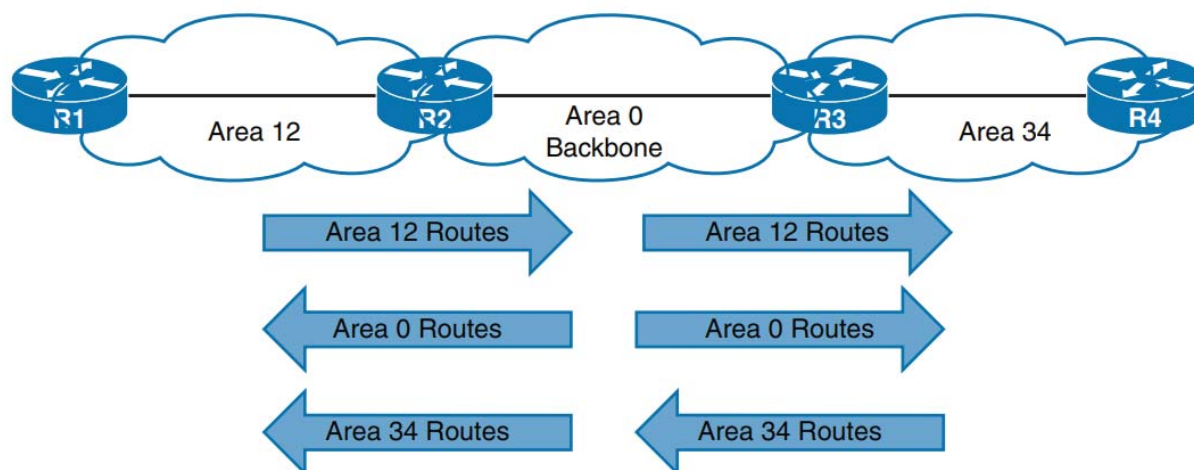


Рис. 6.4. Оголошення маршруту до інших областей

6.5. Протокол BGP

Протокол BGP (Border Gateway Protocol) – це один з головних протоколів маршрутизації в Інтернеті, який використовується для обміну інформацією між різними автономними системами (AS). AS – це незалежні мережі, які використовують BGP для прийняття рішень щодо маршрутизації пакетів даних.

З точки зору BGP, автономна система (AS) є сукупність маршрутизаторів під контролем однієї організації яка використовує один або кілька протоколів внутрішнього шлюзу (IGP). Організація, якій потрібне підключення до Інтернету, повинна отримати ASN. Спочатку ASN склалися з 2 байтів (у 16-біт діапазону), завдяки чому стало можливим 65 535 ASN. Через виснаження, RFC 4893 розширив поле ASN до 4 байтів (32-бітний діапазон). Це дозволяє створити 4 294 967 295 унікальних номерів ASN, забезпечуючи значне збільшення порівняно з початковими 65 535 ASN.

В рамках BGP кожен AS анонсує маршрути, які він може обробляти. Це включає в себе IP-підмережі, які знаходяться в межах цього AS, і

маршрути до інших AS, через які можуть бути доставлені пакети до цих підмереж. Сеанс BGP – це встановлена суміжність між двома BGP маршрутизаторами. Сеанси з кількома переходами вимагають, щоб маршрутизатор використовували основний маршрут, встановлений у інформаційній базі маршрутизації (RIB) (статичного або з будь-якого протоколу маршрутизації), щоб встановити сеанс TCP з віддаленою кінцевою точкою.

Сеанси BGP поділяються на два типи:

- Внутрішній BGP (iBGP): сеанси, встановлені за допомогою маршрутизаторів, iBGP, які знаходяться в тій самій AS.
- Зовнішній BGP (eBGP): сесії, встановлені за допомогою, маршрутизаторів BGP, які знаходяться в іншій AS.

Кожен маршрут в BGP має AS-PATH, який вказує послідовність автономних систем, які пакети пройдуть на шляху до призначення. Це допомагає уникнути петель маршрутизації.

BGP не використовує пакети привітання для виявлення сусідів, як це робиться у протоколах IGP, і він не може динамічно виявляти сусідів. BGP був розроблений як міжавтономний протокол маршрутизації, маючи на увазі, що сусідні межі не повинні змінюватися часто і координуються. BGP-сусіди визначаються IP-адресою.

BGP використовує порт TCP 179 для зв'язку з іншими маршрутизаторами. TCP дозволяє обробляти фрагментацію, послідовність і надійність (підтвердження та повторна передача) пакетів зв'язку. Найновіші реалізації BGP встановіть біт заборони фрагментації (DF), щоб запобігти фрагментації.

BGP використовує TCP, який здатний перетинати мережі (тобто з підтримкою кількох стрибків). У той час як BGP може формувати сусідні суміжності, які є прямими підключеннями, він також може формувати суміжності, які є кількома переходами.

Кожна AS може встановлювати свою власну політику маршрутизації, включаючи фільтрацію, вагу маршрутів та інші правила, які впливають на вибір найкращого маршруту.

Протокол BGP використовує чотири типи повідомлень для обміну інформацією між BGP-маршрутизаторами:

- *OPEN (Відкрити)*: Це перше повідомлення, яке висилається під час встановлення BGP-з'єднання між двома маршрутизаторами. В цьому повідомленні передаються параметри версії BGP, інформація про номер

автономної системи (AS) та інші параметри, необхідні для ініціалізації BGP-з'єднання.

- *UPDATE (Оновити)*: Це повідомлення використовується для анонсування маршрутів та їхніх атрибутів. У повідомленні UPDATE міститься інформація про нові маршрути, або про зміни у вже існуючих маршрутах. Кожен UPDATE-пакет включає в себе інформацію про маршрут, включаючи префікс (IP-адресу та довжину маски), атрибути маршруту і багато іншого.

- *NOTIFICATION (Сповіщення)*: Якщо виникають проблеми під час обміну повідомленнями BGP, то це повідомлення використовується для інформування іншого маршрутизатора про проблему та вимагає завершення BGP-з'єднання. В сповіщенні міститься код помилки та інша інформація, що допомагає іншому маршрутизатору з'ясувати причину проблеми.

- *KEEPALIVE (Підтримка)*: Це повідомлення використовується для підтримки активного BGP-з'єднання. Воно надсилається періодично, щоб підтримувати відкрите BGP-з'єднання, навіть якщо немає активного обміну маршрутами. KEEPALIVE-повідомлення не містять жодних маршрутів чи атрибутів, і вони лише підтверджують, що з'єднання активне.

Протокол BGP має кілька станів сеансу (рис 6.5), які вказують на поточний стан з'єднання між двома BGP-маршрутизаторами. Важливо розуміти ці стани для відладки та аналізу проблем в BGP-з'єднаннях.

Основні стани сеансу BGP:

- *Idle (Неактивний)*: Це початковий стан для BGP-сесії. Маршрутизатор у стані Idle не встановлює з'єднання і не обмінює жодною інформацією BGP з іншими маршрутизаторами.

- *Connect (З'єднання)*: Цей стан вказує на те, що маршрутизатор намагається встановити TCP-з'єднання з іншим маршрутизатором, але з'єднання ще не вдалося встановити.

- *Active (Активний)*: Маршрутизатор перебуває в стані Active, коли він намагається встановити TCP-з'єднання з іншим маршрутизатором, але не отримує відповіді. Це може виникнути через проблеми з доступністю або налаштуваннями.

- *OpenSent (Відкритий відправлено)*: Після успішного встановлення з'єднання, маршрутизатори обмінюють відкриті (OPEN) повідомлення, щоб обговорити параметри сесії.

- *OpenConfirm (Відкритий підтверджено)*: Після обміну відкритими повідомленнями маршрутизатори переходять в стан OpenConfirm для перевірки параметрів сесії. Поки сесія в цьому стані, обмін маршрутами не відбувається.

- *Established (Встановлений)*: Це остаточний стан BGP-сесії. Маршрутизатори вже встановили сесію і можуть обмінюватися маршрутами і оновленнями. В цьому стані сесія діє і пакети маршрутизуються на відповідні маршрути.

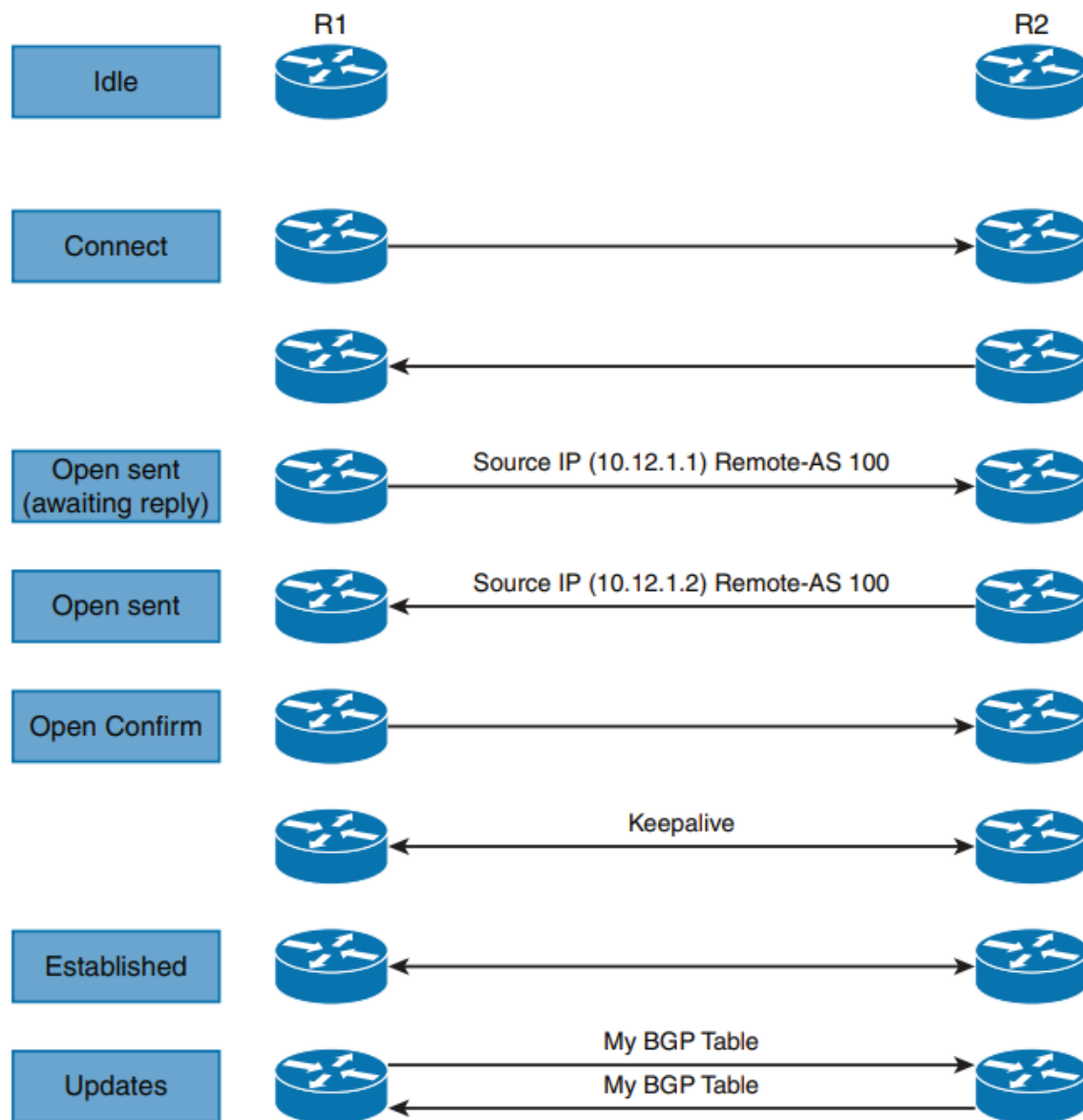


Рис. 6.5. Сусідні стани BGP із встановленням сесії.

Ці стани використовуються для керування та аналізу стану BGP-сесій. У випадку, якщо стан сесії залишається в стані Idle, Connect або Active, це може вказувати на проблеми в BGP-з'єднанні, які потребують подальшого

відладки та розв'язання. Встановлений стан Established означає успішне з'єднання та обмін маршрутами між маршрутизаторами.

6.6. Вибір шляху маршрутизатором

Маршрутизатор визначає шлях, яким повинен пройти пакет, оцінюючи довжину префікса, яка записані в інформаційній базі пересилання (FIB). FIB записується в залежності від даних у таблиці маршрутизації, також відомої як інформаційна база маршрутизації (RIB). RIB складається з найкращих маршрутів, вибраних процесами протоколів маршрутизації.

Вибір шляху має три основні компоненти:

- *Довжина префікса.* Довжина префікса являє собою кількість початкових бітів, виставлених в 1 в масці підмережі.
- *Адміністративна відстань.* Адміністративна відстань (AD) – це рейтинг надійності джерела маршрутної інформації. Якщо маршрутизатор дізнається про маршрут до місця призначення більш ніж з одного протоколу маршрутизації. Якщо всі маршрути мають однакову довжину префікса, тоді порівнюється AD.
- *Метрики.* Метрика – це одиниця вимірювання, яка використовується протоколом маршрутизації для кращого шляху. Метрики відрізняються в різних протоколах маршрутизації.

Давайте розглянемо сценарій, у якому маршрутизатор вибирає маршрут, коли до пункту призначення пакета кілька маршрутів. Припустимо, що маршрутизатор має такі маршрути з різними довжинами префіксів у таблиці маршрутизації:

10.0.3.0/28

10.0.3.0/26

10.0.3.0/24

Кожен із цих маршрутів, також відомий як префіксний маршрут або просто префікс, має свою довжину (маску підмережі). Маршрути вважаються різними пунктами призначення, і всі вони будуть записані в RIB, в так звану таблицю маршрутизації. Таблиця маршрутизації також включає вихідний інтерфейс і IP-адресу наступного переходу (якщо префікс не є безпосередньо під'єднаною мережею). В таблиці 6.1 показано таблицю маршрутизації.

Якщо пакет необхідно переслати, то вибраний маршрут залежить від довжини префікса, де найдовша довжина префікса завжди краща. Наприклад,

/28 краще /26, а /26 краще /24. Нижче наведено приклад, який використовує таблицю 6.1:

Таблиця 6.1.

Приклад таблиці маршрутизації

<i>Prefix</i>	<i>IP Address Range</i>	<i>Next Hop</i>	<i>Outgoing Interface</i>
10.0.3.0/28	10.0.3.0–10.0.3.15	10.1.1.1	Gigabit Ethernet 1/1
10.0.3.0/26	10.0.3.0–10.0.3.63	10.2.2.2	Gigabit Ethernet 2/2
10.0.3.0/24	10.0.3.0–10.0.3.255	10.3.3.3	Gigabit Ethernet 3/3

- Якщо пакет необхідно переслати на 10.0.3.42, маршрутизатор зіставляє 10.0.3.0/24 та префікс 10.0.3.0/26. Але пакет пересилається на 10.2.2.2 з вихідним інтерфейсом Gigabit Ethernet 2/2, тому що 10.0.3.0/26 має найдовший збіг префікса.

- Якщо пакет необхідно переслати на 10.0.3.100, то відповідає лише 10.0.3.0/24 префікс. Пакет переадресований на 10.3.3.3 із вихідним інтерфейсом GigabitEthernet 3/3.

Рішення про пересилання є функцією FIB та є результатом виконаних розрахунків у RIB. RIB розраховує найкращий маршрут на основі комбінації метрик протоколу маршрутизації та адміністративної відстані (AD).

Оскільки кожен протокол маршрутизації отримує оновлення маршрутизації та іншу маршрутну інформацію, він вибирає найкращий шлях до заданого місця призначення та записує цей шлях до таблиці маршрутизації. У таблиці 6.2 представлені AD за замовчуванням для різних протоколів маршрутизації.

Записи в RIB вибираються із різних процесів протоколів маршрутизації. Кожен протокол маршрутизації представляє ту саму інформацію для запису в RIB: мережу призначення, IP-адресу наступного переходу (Next Hop), AD і значення метрик. RIB приймає чи відхиляє маршрут на основі наступної логіки:

- Якщо маршрут не існує у RIB, він приймається.
- Якщо маршрут існує в RIB, необхідно порівняти AD. Якщо AD маршруту в RIB нижче, ніж процес, що надсилає новий маршрут, маршрут відхиляється.
- Якщо маршрут існує в RIB, необхідно порівняти AD. Якщо AD маршруту в RIB вище, ніж процес маршрутизації, що надсилає альтернативну запис, маршрут приймається.

Таблиця 6.2.

Адміністративні відстані протоколів
маршрутизації за замовчуванням

<i>Routing Protocol</i>	<i>Default Administrative Distance</i>
Connected	0
Static	1
EIGRP summary route	5
External BGP (eBGP)	20
EIGRP (internal)	90
OSPF	110
IS-IS	115
RIP	120
EIGRP (external)	170
Internal BGP (iBGP)	200

Розглянемо ще один приклад на цю тему. Припустимо, що маршрутизатор має OSPF, IS-IS і EIGRP. Усі три протоколи дізналися про мережу призначення 10.3.3.0/24 з різними найкращими шляхами та метрикою. Кожен із цих трьох протоколів намагається встановити маршрут до 10.3.3.0/24 у RIB. Оскільки довжина префікса однакова, наступним кроком прийняття рішення є AD, де маршрут протоколу маршрутизації з найменшим AD записується в RIB. Оскільки внутрішній маршрут EIGRP має найкращий AD, він записується в таблицю, як показано в таблиці 6.3.

Таблиця 6.3.

Вибір маршруту для RIB

<i>Routing Protocol</i>	<i>AD</i>	<i>Network</i>	<i>Installs in the RIB</i>
EIGRP	90	10.3.3.0/24	✓
OSPF	110	10.3.3.0/24	X
IS-IS	115	10.3.3.0/24	X

Протокол або протоколи маршрутизації, яким не вдалося записати свій маршрут до таблиці (у даному прикладі OSPF та IS-IS) чекають і повідомляють процесу таблиці маршрутизації, що він повинен повідомити їх, якщо кращий маршрут перестане існувати, щоб вони могли спробувати перевстановити цей маршрут.

Наприклад, маршрут EIGRP 10.3.3.0/24, записаний у таблиці маршрутизації зникає, тоді процес таблиці маршрутизації викликає OSPF та IS-IS і просить їх перевстановити маршрут таблиці маршрутизації. З цих двох протоколів кращий маршрут вибирається з урахуванням AD. Це буде OSPF через його більш низький AD.

Розуміння порядку обробки даних маршрутизатором має вирішальне значення, оскільки в деяких сценаріях шлях із найменшим AD не завжди може бути встановлений у RIB. Наприклад, шлях BGP процес вибору може вибрати шлях iBGP замість eBGP. Таким чином, BGP представить шлях з AD 200, а не 20, RIB, який може не витіснити маршрут, отриманий через OSPF з AD 110.

Логіка вибору найкращого шляху для протоколу маршрутизації може бути різною. Більшість IGP віддають перевагу внутрішнім вивченим маршрутам у порівнянні з зовнішніми маршрутами та подальшому пріоритету шляху з найменшою метрикою. Якщо протокол маршрутизації ідентифікує декілька шляхів як найкращий шлях і підтримує декілька записів шляхів, маршрутизатор встановлює максимальну кількість шляхів, дозволених для кожного пункту призначення. Це відоме як багатошляхове з'єднання з рівною вартістю (Equal-cost multi-path routing ECMP) і забезпечує розподіл навантаження по всіх каналах. EIGRP, OSPF та IS-IS підтримують ECMP. ECMP надає механізм збільшення пропускної спроможності по кількох шляхах шляхом рівномірного поділу трафіку каналами.

На рис.6.5 показано чотири маршрутизатори, на яких працює OSPF.

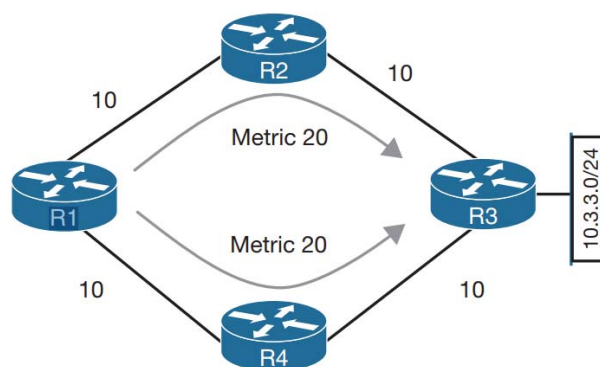


Рисунок 6.5. Технологія OSPF ECMP

Усі чотири маршрутизатори належать одній області та використовують однакову вартість метрики інтерфейсу. R1 має два шляхи з однаковою вартістю для досягнення R3 в мережу 10.3.3.0/24. R1 встановлює обидва

маршрути в таблицю маршрутизації та перенаправляє трафік через шляхи R1-R2-R3 та R1-R4-R3 для доступу до мережі 10.3.3.0/24.

6.7. Статична маршрутизація

Статичні маршрути забезпечують точний контроль за маршрутизацією, але можуть забирати багато часу при адмініструванні. У міру зростання кількості маршрутизаторів та мережевих сегментів використання статичної маршрутизації вимагає більш складного адміністративного ручного контролю. При статичній маршрутизації маршрутизатори не обмінюються даними автоматично, мережевий інтелект відсутній. Якщо маршрут виходить з ладу, інші маршрутизатори не знатимуть, що шлях до мережі недійсний.

Статична маршрутизація має такі характеристики:

- Статичний маршрут налаштовується вручну.
- Адміністратору необхідно переналаштувати статичний маршрут, якщо відбулася зміна топології і статичний маршрут вже нежиттєздатний.
- Статична маршрутизація підходить для невеликої мережі та коли резервних посилань мало або вони відсутні.
- Статична маршрутизація зазвичай використовується з протоколом динамічної маршрутизації для налаштування маршруту за замовчуванням.
- Статичні маршрути корисні, коли:
- Протоколи динамічної маршрутизації не можна використовувати на маршрутизаторі через обмежене використання ЦП маршрутизатора або пам'яті
- Маршрути, отримані з протоколів динамічної маршрутизації, слід замінити статичними.

Статичні маршрути можуть бути класифіковані як:

- Безпосередньо підключені статичні маршрути
- Рекурсивний статичний маршрут
- Повністю визначений статичний маршрут

Послідовним інтерфейсам типу «точка-точка» (P2P) не потрібно турбуватися про збереження суміжності і вони не використовують протокол вирішення адрес (ARP), тому статичні маршрути можуть прямо посилатися на вихідний інтерфейс маршрутизатора. Статичний маршрут, що використовує тільки вихідний маршрут next-hop інтерфейс називається статичним маршрутом з прямим підключенням і вимагає, щоб вихідний інтерфейс перебував у робочому стані для запису маршруту RIB. Рисунок 6.6

ілюструє підключення маршрутизатора R1 до R2 маршрутизатора за допомогою послідовного з'єднання. R1 використовує безпосередньо підключений статичний маршрут до мережі 10.22.22.0/24, а R2 використовує безпосередньо підключений статичний маршрут до мережі 10.11.11.0/24, щоб забезпечити зв'язок між двома віддаленими мережами.

Статичні маршрути необхідно встановлювати на обох маршрутизаторах, щоб зворотньому трафіку був відомий шлях.

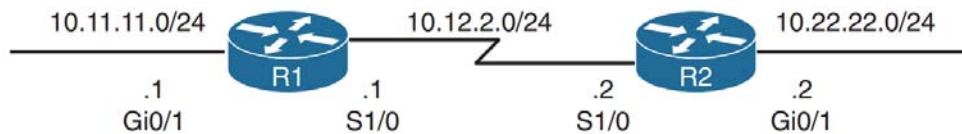


Рисунок 6.6. R1 та R2, з'єднані послідовним з'єднанням

6.8. Статичні маршрути IPv6

Принципи статичної маршрутизації для маршрутів IPv6 такі самі, як і для IPv4.

На рис.6.7 показано маршрутизатори R1 та R2 з адресацією IPv6 для демонстрації статичної маршрутизації.

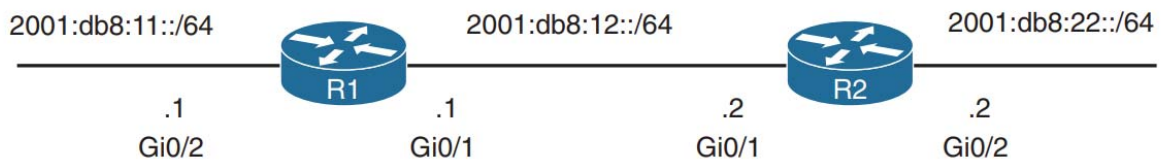


Рисунок 6.7. Топологія статичного маршрута IPv6

Для R1 потрібен статичний маршрут до мережі 2001:db8:22::/64 R2, а для R2 потрібен статичний маршрут до мережі 2001:d8:11::/64.

Контрольні запитання

1. Що таке динамічний протокол маршрутизації, і які переваги він має порівняно зі статичним маршрутизацією?
2. Які є основні типи метрик для вимірювання якості маршруту в динамічних протоколах маршрутизації? Які метрики використовуються в OSPF та EIGRP?

3. Що означає термін "стани сеансу BGP," і які є різниці між цими станами?
4. Порівняйте OSPF та RIP. Які вони мають відмінності у виборі маршруту та підходах до маршрутизації?
5. Як працює алгоритм вибору маршруту в динамічних протоколах маршрутизації? Які етапи включає цей алгоритм?
6. Які типи повідомлень використовуються в протоколі BGP? Для чого призначені OPEN, UPDATE, NOTIFICATION та KEEPALIVE повідомлення?
7. В чому полягає відмінність між статичними та динамічними маршрутами? Які випадки використання підходять до кожного типу маршрутизації?
8. Яким чином протокол OSPF визначає найкоротший шлях до маршруту? Які основні кроки процесу маршрутизації в OSPF?
9. Що таке автономні області (areas) в OSPF, і для чого вони використовуються?
10. Які фактори впливають на вибір протоколу маршрутизації в мережі? Як вибрати найбільш підходящий протокол для конкретної мережі?

РОЗДІЛ 7. СТАНДАРТНІ СТЕКИ КОМУТАЦІЙНИХ ПРОТОКОЛІВ

Взаємодія комп'ютерів в мережах відбувається відповідно до певних правил обміну повідомленнями і їхніми форматами, тобто відповідно до певних протоколів. Ієрархічно організована сукупність протоколів, що вирішує завдання взаємодії вузлів мережі, називається стеком комунікаційних протоколів.

Існує досить багато стеків протоколів, широко застосовуваних в мережах [17; 39; 45]. Це і стеки, що є міжнародними та національними стандартами, і фірмові стеки, що одержали поширення завдяки поширеності обладнання тої або іншої фірми. Прикладами популярних стеків протоколів можуть служити стек IPX/SPX фірми Novell, стік TCP/IP, використовуваний в мережі Internet і в багатьох мережах на основі операційної системи UNIX, стек OSI міжнародної організації по стандартизації, стек DECnet корпорації Digital Equipment і деякі інші.

Використання в мережі того або іншого стека комунікаційних протоколів багато в чому визначає тип мережі і її характеристики. У невеликих мережах може використовуватися винятково один стек. У великих корпоративних мережах, що поєднують різні мережі, паралельно використовуються, як правило, декілька стеків.

У комунікаційному встаткуванні реалізуються протоколи нижніх рівнів, які краще стандартизовані, ніж протоколи верхніх рівнів, і це є передумовою для успішної спільної роботи обладнання різних виробників. Перелік протоколів, підтримуваних тим або іншим комунікаційним пристроєм, є однієї з найбільш важливих характеристик цього пристрою.

Комп'ютери реалізують комунікаційні протоколи у вигляді відповідних програмних елементів мережної операційної системи, наприклад, протоколи каналного рівня, як правило, виконані у вигляді драйверів мережних адаптерів, а протоколи верхніх рівнів у вигляді серверних і клієнтських компонентів мережних сервісів.

Уміння ефективно працювати в середовищі тої або іншої операційної системи є важливою характеристикою комунікаційного обладнання. Часто можна прочитати в рекламі мережного адаптера або концентратора, що він розроблявся спеціально для роботи в мережі NetWare або UNIX. Це означає, що розроблювачі апаратури оптимізували її характеристики стосовно до тих протоколів, які використовуються в цій мережній операційній системі, або до

даної версії їхньої реалізації, якщо ці протоколи використовуються в різних ОС. Через особливості реалізації протоколів у різних ОС, у якості однієї з характеристик комунікаційного обладнання використовується сертифікованість на можливість роботи в середовищі даної ОС.

На нижніх рівнях – фізичному та канальному – практично у всіх стеках використовуються ті самі протоколи. Це добре стандартизовані протоколи Ethernet, Token Ring, FDDI і деякі інші, які дозволяють використовувати у всіх мережах ту саму апаратуру.

Протоколи мережного й більш високих рівнів існуючих стандартних стеків відрізняються великою різноманітністю і, як правило, не відповідають розбивці, що рекомендується моделлю ISO. Зокрема, в цих стеках функції сеансового та представницького рівня найчастіше об'єднані із прикладним рівнем. Така невідповідність пов'язана з тим, що модель ISO з'явилась як результат узагальнення вже існуючих і реально використовуваних стеків, а не навпаки.

7.1. Стек TCP/IP

Стек протоколів TCP/IP був розроблений на початку 80-х років XX сторіччя за ініціативою Міністерства оборони США як набір протоколів для різноманітної складної мережі. Сьогодні цей стек є, мабуть, одним з найпопулярніших і використовується для зв'язку мільйонів комп'ютерів у всесвітній мережі Інтернет, а також великої кількості телекомунікаційних мереж.

7.1.1. Реалізація міжмережної взаємодії засобами TCP/IP

Багаторівнева структура стека TCP/IP. Стек TCP/IP [3,5-7] розроблений до появи моделі OSI, тому відповідність рівнів стека TCP/IP рівням моделі OSI достатньо умовна. У стеку TCP/IP визначено 4 рівні: прикладний, транспортний, міжмережевої взаємодії і мережевих інтерфейсів (табл. 7.1).

Прикладний рівень стека відповідає трьом верхнім рівням моделі OSI. За довгі роки стек TCP/IP увібрав в себе велику кількість протоколів і служб прикладного рівня. До них відносяться такі популярні протоколи як протокол копіювання файлів (FTP), протокол емуляції терміналу (telnet), протокол передачі електронної пошти (SMTP), протокол передачі гіпертекстової інформації (HTTP) і багато інших. Протоколи прикладного рівня

встановлюються на кінцевих вузлах (за термінологією Інтернет – на хостах), відпрацьовують логіку програм і звертаються до протоколів нижніх рівнів як до набору інструментів для передачі інформації по мережі.

Таблиця 7.1

Структура стека TCP/IP

Рівні OSI	Рівні стеку TCP/IP	Протоколи, які підтримують стек TCP/IP
Прикладний	Прикладний	FTP, telnet, SNMP, SMTP, HTTP, TFTP
Представницький		
Сеансовий		
Транспортний	Транспортний	TCP, UDP
Мережевий	Рівень міжмережної взаємодії	IP, RIP, OSPF, ICMP
Канальний	Рівень мережесих інтерфейсів	Сімейство Ethernet, Token Ring, FDDI, PPP, SLIP, X.25, ISDN, FR, ATM
Фізичний		

Транспортний рівень стека включає протоколи TCP і UDP, які також встановлюються на хостах. Цим протоколам відводиться роль сполучної ланки між протоколами прикладного рівня і протоколами рівня міжмережесої взаємодії. Від прикладного протоколу транспортний рівень отримує завдання на передачу даних з тією або іншою якістю. До нижнього рівня транспортні протоколи звертаються для передачі пакету по мережі.

Протокол TCP забезпечує надійну гарантовану доставку даних. Якщо таке завдання не ставиться перед засобами транспортного рівня, то використовується простий дейтаграмний протокол UDP.

Рівень міжмережесої взаємодії стека TCP відповідає мережевому рівню моделі OSI. Основним протоколом цього рівня є протокол IP. Його головне завдання – забезпечити передачу пакету між підмережами до тих пір, поки він не потрапить в мережу призначення. Цей протокол встановлюється не тільки на хостах, але і на всіх маршрутизаторах.

До рівня міжмережесої взаємодії відносяться також протоколи збору маршрутної інформації (RIP, OSPF) і протокол міжмережесих повідомлень ICMP, що управляють, призначеною для обміну службовою інформацією між маршрутизаторами мережі і вузлом-джерелом пакету. За допомогою

спеціальних пакетів ICMP повідомляє про неможливість доставки пакету, про перевищення часу його життя, про які-небудь зміни, що виникли при обслуговуванні і т.п.

Рівень мережесих інтерфейсів в стеку TCP/IP не регламентується. Проте цей стек на нижньому рівні підтримує всі популярні стандарти фізичного і канального рівнів. Це протоколи локальних мереж сімейства Ethernet, Token Ring, FDDI, протоколи глобальних мереж PPP, SLIP, X.25, ISDN, FR, ATM.

Хоча стек TCP/IP тісно пов'язаний з мережею Інтернет, існує велика кількість мереж, які не входять до складу цієї усесвітньої інформаційної мережі, але теж використовують цей популярний стек. Такі мережі називають IP-мережами. Основними протоколами стека, що визначають його специфіку і назву, є протоколи TCP і IP, які детально будуть розглянуті нижче.

7.1.2. Типи адрес стеку TCP/IP

З огляду на тенденцію швидкого росту мережі Internet, в основу якої покладений TCP/IP, розроблений стек протоколів TCP/IP версії 6, що використовується поки не настільки значних масштабах. Основу нової версії стека протоколів становить *протокол міжмережної взаємодії нового покоління* (IP new generation, IPng або IPv6). У даному підрозділі буде розглядатися тільки TCP/IP версії 4.

Протокол міжмережної взаємодії (IP) є протоколом мережного рівня. Цей протокол визначає спосіб адресації мереж і окремих вузлів і забезпечує підтримку маршрутизації потоків даних.

Кожному вузлів мережі TCP/IP (хосту) призначається 32-розрядна логічна адреса, названа IP-адресою і складається в загальному випадку із двох полів – адреси (номер) мережі та адреси (номер) вузла. Адреса мережі унікально ідентифікує кожну мережу і призначається централізовано. Якщо мережа підключена до Internet, адресу мережі може бути отримано безпосередньо в мережному інформаційному центрі (Internet Network Information Center, InterNIC) або ж призначений регіональним провайдером послуг Internet (ISP), що отримали блок адрес в InterNIC. Адреса хосту вибирається адміністратором мережі, але повинна бути унікальною у межах мережі. Для запису IP-адреси найчастіше використовується десяткова форма запису з поділяючими точками (dotted decimal notation), відповідно до якої

кожний октет представляється десятковим числом у діапазоні від 0 до 255, наприклад, 1.2.3.4. Загальний формат IP-адреси представлений на рис. 7.1.

Для виділення з IP-адреси номера мережі і номеру вузла, були визначені 5 класів адрес – класи А, В, С, D і Е. Для загального користування були доступні тільки класи А, В і С. Клас D призначався для використання в мережах із груповою адресацією, клас Е був зарезервований для подальшого використання.

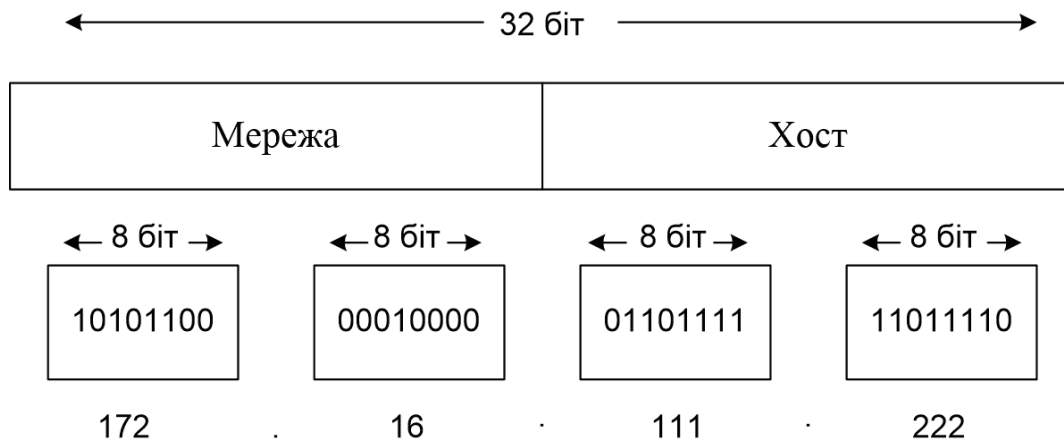


Рис. 7.1. Загальний формат IP-адреса

Формат адреси для мереж класів А, В і С наведений на рис. 7.2.

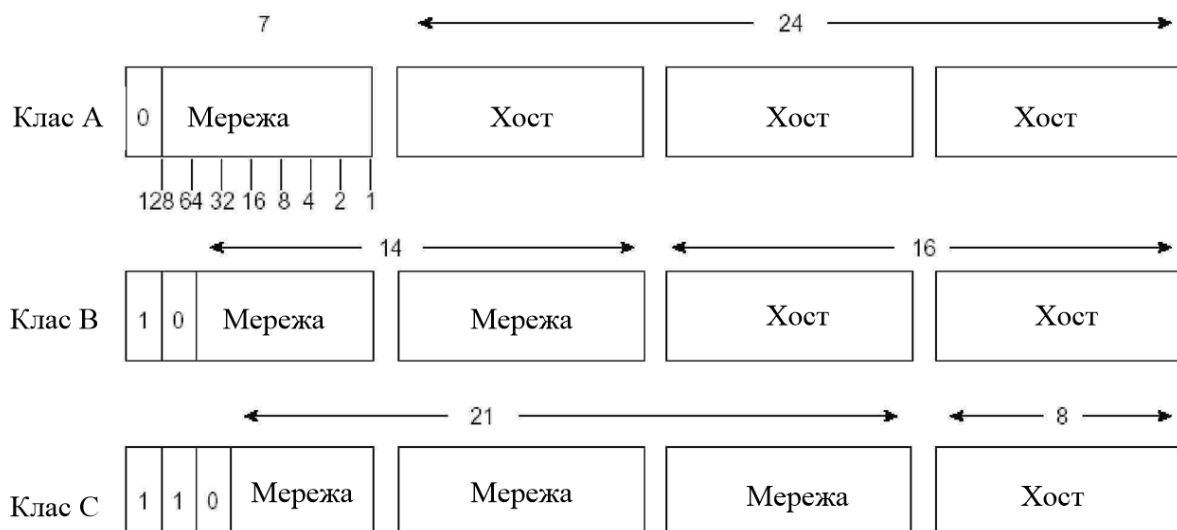


Рис. 7.2. Формат адрес для мереж класів А, В і С

Клас IP-адреси, а, отже, і співвідношення між розмірностями полів номера мережі і номера вузла, можуть бути легко визначені за старшими

бітами першого октету. Основні характеристики мереж різних класів наведені в табл. 7.2.

Таблиця 7.2

Основні характеристики мереж різних класів

Клас адреси	Формат адреси	Старші біти	Діапазон адрес	Кількість біт в адресі мережі / хоста	Кількість мереж	Кількість хостів в мережі
A	C.X.X.X	0	1.0.0.0	7/24	126	16 777 214
B	C.C.X.X	10	128.1.0.1	14/16	16384	65 543
C	C.C.C.X	110	192.0.0.0 223.255.254.0	22/8	4194304	254
D	Не визначено	1110	224.0.0.0 239.255.255.255	Не визначено	Не визначено	Не визначено
E	Не визначено	1111	224.0.0.0 254.255.255.255	Не визначено	Не визначено	Не визначено

Деякі IP-адреси мають спеціальне призначення і не можуть бути використані для вузлів у реальних мережах (табл. 7.3).

Таблиця 7.3

Спеціальні призначення IP-адрес

Тип адреси		Призначення
Всі нулі	0.0.0.0	Даний вузол
[Номер мережі].[Всі нулі]	192.168.1.0	Дана мережа
[Всі нулі].[Номер вузла]	0.0.0.1	Вузол даної мережі
Всі одиниці	255.255.255.255	Всі вузли даної мережі
[Номер мережі].[Всі одиниці]	192.168.1.255	Всі вузли зазначеної мережі
127.[Будь-яке число]	127.0.0.1	“Петля” (loopback)

Для використання в частинах (внутрішніх) мережах зарезервовані три блоки IP-адрес:

10.0.0.0 – 10.255.255.255

172.16.0.0 – 172.31.255.255

192.168.1.0 – 192.168.255.255

Ці адреси призначені для внутрішнього використання і можуть призначатися вузлам у будь-якій мережі без попереднього узгодження з якою-небудь організацією. Очевидно, що ці адреси не є унікальними в межах глобальної мережі, тому не можуть бути використані для адресації хостів з інших мереж. Зовнішні мережні шлюзи й маршрутизатори відкидають всі пакети, що відправляються хостами, у яких є тільки внутрішні адреси.

IP-мережа може бути розбита на більш дрібні фрагменти, називані підмережами. Кожна підмережа представляється як звичайна IP-мережа, що надає велику гнучкість схемі розподілу адрес, дозволяє більш ефективно витрачати адреси і уникнути їх порожньої втрати. Перевагою використання підмереж є також те, що для зовнішнього світу мережа організації представляється як єдине ціле, завдяки чому ховається її реальна внутрішня структура.

Для завдання номера підмережі виділяється деяка частина розрядів з поля номера вузла. Розмірність поля номера підмережі змінюється залежно від необхідної кількості підмереж і кількості вузлів у кожній з них. Для виділення номера підмережі використовується *маска підмережі* (subnet mask). Формат маски підмережі аналогічний формату IP-адреси. Однак, маска підмережі у двійковому поданні завжди містить послідовність “1” у тій частині, що відповідає номеру мережі і підмережі, і послідовність “0” у тій частині, що відповідає номеру вузла (рис. 7.3).



Рис. 7.3. Маска підмережі

Для мереж класів А, В і С у випадку відсутності підмереж використовуються маски 255.0.0.0, 255.255.0.0 і 255.255.255.0 відповідно. При необхідності використання підмереж потрібно визначити кількість розрядів у полях номера під мережі і номера вузла. Помітимо, що номера підмереж, що складаються із всіх “0” або “1”, використовувати, як правило,

не рекомендується. Для розрахунку можна скористатися одним з наступних способів:

1. Виходячи з необхідності, задається кількість підмереж i^* . Довжина поля номера підмережі визначається за формулою $n_s = |\log_2(N_s + 2)|$. Поле номера вузла буде мати розмірність $n_h = 32 - (n_n + n_s)$ розрядів, де n_n – довжина поля номера мережі. Отже, максимальна кількість хостів у кожній підмережі дорівнює

$$N_h = 2^{n_h} - 2.$$

2. Виходячи з необхідності, задається максимальна кількість вузлів у кожній підмережі N_h . Довжина поля номера вузла визначається за формулою

$$n_h = |\log_2(N_h + 2)|.$$

Поле номера підмережі буде мати розмірність $n_s = 32 - (n_n + n_h)$ розрядів, де n_n – довжина поля номера мережі. Отже, максимальна кількість підмережі дорівнює $N_s = 2^{n_s} - 2$. У цьому випадку передбачається, що у всіх підмережах використовуються однакові (рівні) маски. Це може виявитися неприйнятним у тому випадку, коли кількість вузлів у різних підмережах істотно розрізняється.

Для усунення цього недоліку можуть бути використані нерівні маски або маски змінної довжини (variable length subnet mask). У цьому випадку процес розбивки мережі на підмережі виконується в кілька етапів, коли на першому етапі розбивається базова мережа, а надалі отримані підмережі у свою чергу розбиваються на підмережі.

Наприклад, припустимо, що мережі організації надана IP-адреса 172.16.0.0. Необхідно визначити 10 підмереж однакового розміру. У такому випадку для завдання номера підмережі буде потрібно виділити 4 біти з поля номера вузла, що дозволить адресувати до 16 підмереж. Маска для кожної підмережі буде задаватися у вигляді 255.255.240.0. Кожна підмережа дозволяє адресувати 16382 вузла. Адреси підмереж наведені в табл. 7.4.

В іншому випадку, припустимо, організації надана адреса 192.168.1.0. Адреси необхідно розподілити між п'ятьма взаємозалежними мережами, у трьох з яких є 50 вузлів, у двох залишилися по 30. Очевидно, що, використовуючи рівні маски підмережі, не можна одержати рішення, що задовільняє умовам задачі. Тому необхідно скористатися масками змінної довжини.

На першому етапі при використанні маски підмережі 255.255.255.192 мережа розбивається на чотири підмережі, у кожній з яких може перебувати до 64 хостів (табл. 7.5).

Таблиця 7.4.

Адреси підмереж

№	Адреса підмережі	Адреса ширококомовної передачі для підмережі
1.	172.16.0.0	172.16.15.255
2.	172.16.16.0	172.16.31.255
3.	172.16.32.0	172.16.47.255
4.	172.16.48.0	172.16.63.255
5.	172.16.64.0	172.16.79.255
6.	172.16.80.0	172.16.95.255
7.	172.16.96.0	172.16.111.255
8.	172.16.112.0	172.16.127.255
9.	172.16.128.0	172.16.143.255
10.	172.16.144.0	172.16.159.255
11.	172.16.160.0	172.16.175.255
12.	172.16.176.0	172.16.191.255
13.	172.16.192.0	172.16.207.255
14.	172.16.208.0	172.16.223.255
15.	172.16.224.0	172.16.239.255
16.	172.16.240.0	172.16.255.255

Таблиця 7.5.

Підмережі маски 255.255.255.192

№	Адреса підмережі	Маска підмережі	Адреса ширококомовної передачі для підмережі
1.	192.168.1.0	255.255.255.192	192.168.1.63
2.	192.168.1.64	255.255.255.192	192.168.1.127
3.	192.168.1.128	255.255.255.192	192.168.1.191
4.	192.168.1.192	255.255.255.192	192.168.1.255

Після цього одна з отриманих підмереж за допомогою маски 255.255.255.224 розбивається ще на дві підмережі по 32 вузла в кожній (табл. 7.6).

Таблиця 7.6.

Підмережі маски 255.255.255.224

№	Адреса підмережі	Маска підмережі	Адреса широкомовної передачі для підмережі
1.	192.168.1.0	255.255.255.192	192.168.1.63
2.	192.168.1.64	255.255.255.192	192.168.1.127
3.	192.168.1.128	255.255.255.192	192.168.1.191
4.	192.168.1.192	255.255.255.224	192.168.1.223
5.	192.168.1.224	255.255.255.224	192.168.1.255

У даному прикладі задіяні підмережі, номери яких у двійковому поданні містять всі “0” і “1”, що може виявитися неприйнятним при наявності апаратних або програмних маршрутизаторів, що не підтримують безкласову маршрутизацію.

Важливою функцією мережного рівня є управління процесом маршрутизації пакетів, переданих через мережу. Для з’єднання джерела і одержувача повинен бути встановлений маршрут або набір маршрутів. Зазвичай маршрути фіксуються в кожному вузлі за допомогою записів у відповідній таблиці маршрутів, що показує по якому вихідному каналу повинен направлятися даний пакет. Алгоритми вибору маршрутів, застосовувані для встановлення відповідних шляхів і формування таблиць маршрутів, ґрунтуються на обліку міри вартості кожного маршруту. Вартість може бути величиною фіксованої і визначатися такими параметрами, як довжина лінії, швидкість передачі або ширина смуги (пропускна здатність), безпека, оцінювана затримка при передачі сигналу і т.п.

Пристрої, що вирішують дану задачу, називаються маршрутизаторами (router). *Маршрутизатори* поєднують окремі мережі в загальну складену мережу. Внутрішня структура кожної мережі в цьому випадку значення не має. До кожного маршрутизатора можуть бути приєднані декілька мереж (принаймні, дві). У складних складених мережах майже завжди існує декілька альтернативних маршрутів для передачі пакетів між двома кінцевими вузлами. *Маршрут* – це шлях (послідовність маршрутизаторів), що повинен пройти пакет від відправника до пункту призначення. Маршрутизатор вибирає маршрут на підставі свого подання про поточну конфігурацію мережі й відповідного критерію вибору маршруту. Зазвичай як критерій виступає час проходження маршруту, що у локальних мережах

збігається з довжиною маршруту, вимірюваної в кількості пройдених вузлів маршрутизації (у глобальних мережах приймається в розрахунок і час передачі пакета по кожній лінії зв'язку).

В мережі Internet, найбільш розвинутою на даний момент мережі дейтаграмного типу, деякі маршрутизатори використовуються для переміщення інформації через одну конкретну групу мереж, що перебувають під тим самим адміністративним початком і управлінням (такий об'єкт називається автономною системою – autonomous system). Маршрутизатори, використовувані для обміну інформацією в межах автономних систем, називаються внутрішніми (interior routers); вони використовують різні протоколи внутрішніх шлюзів (Interior Gateway Protocol, IGP) для виконання задачі. Маршрутизатори, які переміщують інформацію між автономними системами, називаються зовнішніми (exterior routers); для цього вони використовують протоколи зовнішньої маршрутизації (Exterior Gateway Protocol, EGP).

Для нагромадження інформації про поточну конфігурацію мережі маршрутизатори обмінюються маршрутною інформацією між собою за спеціальним протоколом. Протоколи цього типу називаються *протоколами обміну маршрутною інформацією* (або протоколами маршрутизації). Протоколи обміну маршрутною інформацією варто відрізнити від протоколів мережного рівня, оскільки вони служать для обміну службовою інформацією, тоді як протоколи мережного рівня призначені для передачі користувальницьких даних, аналогічно протоколам канального рівня.

Для доставки пакетів протоколу обміну маршрутною інформацією використовується протокол мережного рівня, тому що тільки він може передати інформацію між маршрутизаторами, що перебувають у різних мережах. Пакет протоколу обміну маршрутною інформацією міститься в поле даних пакета мережного рівня. За допомогою протоколів обміну маршрутною інформацією маршрутизатори становлять карту міжмережних зв'язку того або іншого ступеня і ухвалюють рішення щодо того, якому наступному вузлу потрібно передати пакет.

7.1.3. Протоколи обміну маршрутною інформацією стека TCP/IP

Протоколи обміну маршрутною інформацією стека TCP/IP є адаптивними, у свою чергу їх можна розділити на дві групи:

- протоколи вектора відстаней (distance vector);

– протоколи стану зв'язку (link state).

Протоколи, що використовують алгоритм вектора відстаней, пропонують кожному маршрутизатору періодично і широкомовно розсилати по мережі вектор відстаней від себе до всіх відомих йому мереж. Під *відстанню* звичайно розуміється число проміжних маршрутизаторів, через які пакет повинен пройти перш, ніж потрапить у відповідну мережу (hop). Може використовуватися і інша метрика, що враховує не тільки кількість проміжних пунктів, але й час проходження пакетів між сусідніми маршрутизаторами. Одержавши вектор від сусіднього маршрутизатора, кожний маршрутизатор додає до нього інформацію про відомі йому інші мережі, про які він довідався безпосередньо (якщо вони підключені до його портів) або з аналогічних оголошень інших маршрутизаторів, а потім знову розсилає нове значення вектора по мережі. Зрештою, кожний маршрутизатор довідається інформацію про наявні в інтермережі мережі і про відстань до них через сусідні маршрутизатори.

Алгоритми вектора відстаней добре працюють тільки в невеликих мережах. У великих мережах вони засмічують лінії зв'язку інтенсивним широкомовним трафіком, до того ж зміни конфігурації можуть спрацьовуватися за цим алгоритмом не завжди коректно, тому що маршрутизатори не мають точного подання про топологію зв'язку у мережі, а мають у своєму розпорядженні тільки узагальнену інформацію – вектор відстаней, до того ж отриману через посередників. Робота маршрутизатора в цьому випадку нагадує роботу мосту, тому що точної топологічної картини мережі такий маршрутизатор не має.

Найпоширенішим протоколом, заснованим на алгоритмі вектора відстаней, є *протокол RIP* (Routing Information Protocol – протокол інформації маршрутизації), описаний в RFC 1058. Це один з найстарших протоколів обміну маршрутною інформацією, однак, він дотепер надзвичайно розповсюджений в обчислювальних мережах. Існують різновиди протоколу RIP для різних мереж і різних стеків протоколів.

Відповідно до протоколу RIP всі мережі мають номери (спосіб утворення номера залежить від використовуваного в мережі протоколу мережного рівня), а всі маршрутизатори – ідентифікатори. Вектор відстаней являє собою набір пар чисел, що відповідають номерам мереж і відстаням до них. Вектора відстаней ітераційно поширюються маршрутизаторами мережі, і через декілька кроків кожний маршрутизатор має дані про досяжні для нього мережі і про відстані до них. Якщо зв'язок з якою-небудь мережею

обривається, то маршрутизатор відзначає цей факт тим, що привласнює елементу вектора, що відповідає відстані до цієї мережі, максимально можливе значення, що має спеціальний сенс – “зв’язку ні”. Таким значенням у протоколі RIP є число 16.

Кожний запис даних у таблиці маршрутизації RIP містить необхідну інформацію, включаючи кінцевий пункт призначення. У таблиці маршрутизації може перебувати також і інша інформація, у тому числі різні таймери, пов’язані з даним маршрутом. Типова таблиця маршрутизації RIP наведена на рис. 7.4.

Destination	Nexthop	Distance	Timers	Flags
Network A	Router 1	3	11.12.13	x, y
Network B	Router 2	5	11.12.13	x, y
Network C	Router 3	2	11.12.13	x, y
.	.	.	.	.
.	.	.	.	.
.	.	.	.	.

Рис. 7.4. Типова таблиця маршрутизації RIP

RIP зберігає тільки найкращі маршрути до пункту призначення. Якщо нова інформація забезпечує кращий маршрут, то ця інформація замінює стару маршрутну інформацію. Зміни в топології мережі можуть викликати зміни в маршрутах, приводячи до того, наприклад, що який-небудь новий маршрут стає кращим маршрутом до конкретного пункту призначення.

Коли мають місце зміни в топології мережі, то ці зміни відбиваються в повідомленнях про коректування маршрутизації. Наприклад, коли який-небудь маршрутизатор виявляє відмову одного з каналів або іншого маршрутизатора, він повторно обчислює свої маршрути і відправляє повідомлення про коректування маршрутизації. Кожний маршрутизатор, що приймає повідомлення про відновлення маршрутизації, у якому втримується зміна, коректує свої таблиці й поширює цю зміну.

RIP визначає ряд характеристик, призначених для більш стабільної роботи в умовах топології мережі, що швидко змінюється. У їх число входить обмеження кількості пересилань, часові затримки змін (hold-downs),

розщеплені горизонти (split-horizons) і коректування скасування (poison reverse updates).

Обмеження кількості пересилань

RIP дозволяє максимальне число пересилань, рівне 15. Будь-якому пункту призначення, що перебуває далі, ніж на відстані 15 пересилань, привласнюється ярлик “недосяжного”. Максимальне число пересилань RIP значною мірою обмежує його застосування у великих об'єднаних мережах, однак сприяє запобіганню появи проблеми, названої рахунком нескінченності (count to infinity), що приводить до зациклення маршрутів у мережі. Проблема рахунку нескінченності наведена на рис. 7.5.

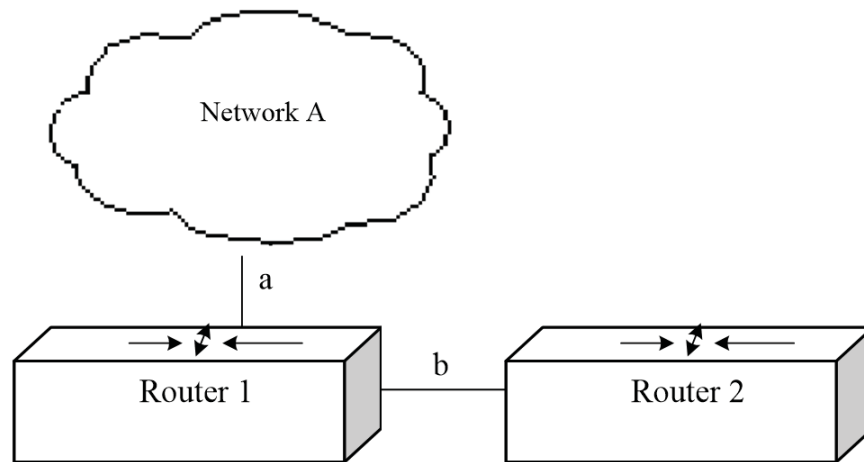


Рис. 7.5. Проблема рахунку нескінченності

Розглянемо, що трапиться, якщо на рис. 7.5 канал *a* маршрутизатора 1 (R1), що зв'язує його з мережею А, відмовить. R1 перевіряє свою інформацію і виявляє, що маршрутизатор 2 (R2) пов'язаний з мережею А каналом довжиною в одне пересилання. Тому що R1 знає, що він прямо з'єднаний з R2, то він повідомляє про маршрут із двох пересилань до мережі А і починає направляти весь трафік у мережу А через R2. Це приводить до утворення маршрутної петлі. Коли R2 виявляє, що R1 може тепер досягти мережу А за два пересилання, воно змінює запис своїх власних даних у таблиці маршрутизації, щоб показати, що він має тракт довжиною в 3 пересилання до мережі А. Ця проблема, а також дана маршрутна петля будуть тривати нескінченно, або доти, поки не буде нав'язана яка-небудь зовнішня гранична умова. Цією граничною умовою є максимальна кількість пересилань RIP. Коли число пересилань перевищить 15, даний маршрут маркірується як недосяжний. Через якийсь час цей маршрут видаляється з таблиці.

Часові затримки змін використовуються для того, щоб перешкодити регулярним повідомленням про коректування, незаконно відновити в правах маршрут, що виявився зіпсованим. Коли який-небудь маршрут відмовляє, сусідні маршрутизатори виявляють це. Потім вони обчислюють нові маршрути і відправляють повідомлення про відновлення маршрутизації, щоб інформувати своїх сусідів про зміни в маршруті. Ця діяльність приводить до появи цілої хвилі корекцій маршрутизації, які фільтруються через мережу.

Приведені в дію коректування неодноразово прибувають в усі пристрої мережі. Тому можливо, що який-небудь пристрій, що ще не одержав інформацію про яку-небудь відмову в мережі, може відправити регулярне повідомлення про коректування (у якому маршрут, що тільки що відмовив, усе ще значиться справним) в інший пристрій, що тільки що одержав повідомлення про цю відмову в мережі. У цьому випадку цей інший пристрій тепер буде мати (і можливо, рекламувати) неправильну маршрутну інформацію.

Команди про часове втримання вказують маршрутизаторам, щоб вони на якийсь час притримали будь-які зміни, які можуть вплинути на тільки що вилучені маршрути. Цей період утримання звичайно розраховується таким чином, щоб він був більше періоду часу необхідного для внесення якої-небудь зміни про маршрутизацію у всю мережу. *Розщеплені горизонти* використовують перевагу того факту, що ніколи не буває корисним відправляти інформацію про який-небудь маршрут назад у тому напрямку, з якого прийшла ця інформація. Для ілюстрації цього положення розглянемо рис. 7.6.

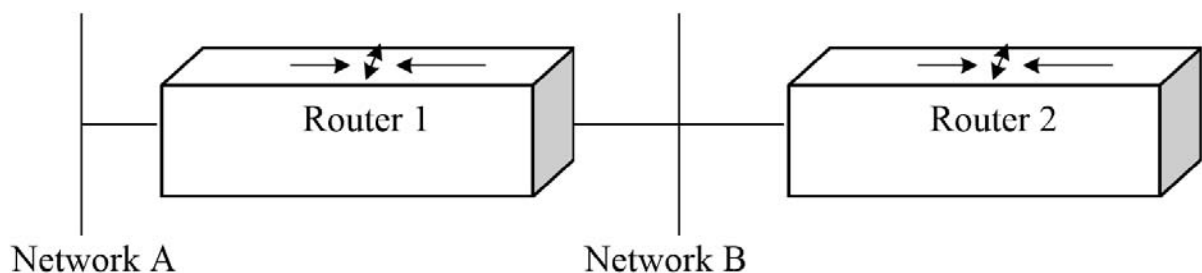


Рис. 7.6. Приклад відправки повідомлення

Маршрутизатор 1 (R1) спочатку повідомляє, що він має у своєму розпорядженні якийсь маршрут до мережі А. Маршрутизатору 2 (R2) немає підстав включати цей маршрут у своє управління, що відсилається назад

маршрутизатору R1, тому що R1 ближче до мережі А. Правило розщепленого горизонту говорить, що R2 повинен виключити (потрапити на) цей маршрут при будь-яких коректуваннях, які він відправляє в R1. Правило розщепленого горизонту допомагає запобігти маршрутним петлям між двома вузлами. Наприклад, розглянемо випадок, коли відмовляє інтерфейс R1 з мережею А.

При відсутності розщеплених горизонтів R2 продовжує інформувати R1 про те, що він може потрапити в мережу А через R1. Якщо R1 не має у своєму розпорядженні достатній інтелект, то він дійсно може вибрати маршрут, пропонується R2, як альтернатива для свого прямого зв'язку, який відмовил, що приводить до утворення петлі маршрутизації. І хоча тимчасове утримання змін повинне запобігати це, застосування розщепленого горизонту забезпечує додаткову стабільність алгоритму.

Коректування відміни маршруту

У той час як задачею розщеплених горизонтів є запобігання утворення маршрутних петель між сусідніми маршрутизаторами, коректування відміни призначені для усунення великих маршрутних петель. В основі їх дії лежить положення про те, що збільшення значення показників маршрутизації звичайно вказує на наявність маршрутних петель. У цьому випадку відправляються коректування відміни для видалення даного маршруту і приведення його в стан тимчасового утримання. Протокол RIP використовує евристичний алгоритм Белмана-Форда, і рішення, знайдене з його допомогою є не оптимальним, а близьким до оптимального.

Перевагою протоколу RIP є його обчислювальна простота, а недоліками – збільшення трафіку при періодичному розсиланні широкомовних пакетів і неоптимальність знайденого маршруту.

На рис. 7.7 наведений випадок нестійкої роботи мережі за протоколом RIP при зміні конфігурації – відмові лінії зв'язку маршрутизатора M1 з мережею 1. При працездатному стані цього зв'язку в таблиці маршрутів кожного маршрутизатора є запис про мережу з номером 1 і відповідною відстанню до неї.

При обриві зв'язку з мережею 1 маршрутизатор M1 відзначає, що відстань до цієї мережі прийняла значення 16. Однак одержавши через якийсь час від маршрутизатора M2 маршрутне повідомлення про те, що від нього до мережі 1 відстань становить 2 пересилання, маршрутизатор M1 нарощує цю відстань на 1 і відзначає, що мережа 1 досяжна через маршрутизатор 2. В результаті пакет, призначений для мережі 1, буде циркулювати між маршрутизаторами M1 і M2 доти, поки не мине час зберігання запису про

мережу 1 у маршрутизаторі 2, і він не передасть цю інформацію маршрутизатору M1.

Для виключення подібних ситуацій маршрутна інформація про відомий маршрутизатор мережі не передається тому маршрутизатору, від якого вона прийшла.

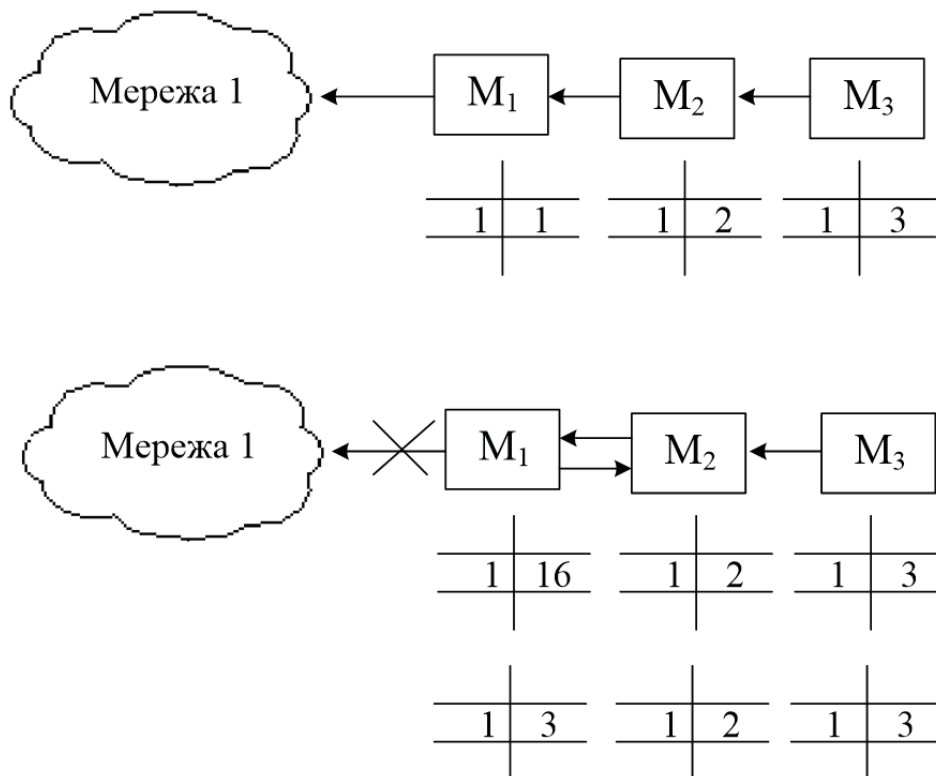


Рис. 7.7. Випадок нестійкої роботи мережі

Існують і інші, більш складні випадки нестабільного поведіння мереж, що використовують протокол RIP, при змінах у стані зв'язку або маршрутизаторів мережі.

Алгоритми стану зв'язку забезпечують кожний маршрутизатор інформацією, достатньої для побудови точного графа зв'язку мережі. Всі маршрутизатори працюють на підставі однакових графів, що робить процес маршрутизації більш стійким до змін конфігурації. Широкомовне розсилання використовується тут тільки при змінах стану зв'язку, що відбувається в надійних мережах не так часто.

Для того, щоб зрозуміти, у якому стані перебувають лінії зв'язку, підключені до його портів, маршрутизатор періодично обмінюється короткими пакетами зі своїми найближчими сусідами. Цей трафік також широкомовний, але він циркулює тільки між сусідами й тому не так засмічує мережу.

Протоколом, заснованим на алгоритмі стану зв'язку, у стеці TCP/IP є *протокол OSPF* (Open Shortest Path First), який володіє багатьма особливостями, орієнтованими на застосування у великих гетерогенних мережах.

Протокол OSPF обчислює маршрути в IP-мережах, зберігаючи при цьому інші протоколи обміну маршрутною інформацією.

Безпосередньо зв'язані (тобто досяжні без використання проміжних маршрутизаторів) маршрутизатори називаються “сусідами”. Кожний маршрутизатор зберігає інформацію про те, у якому стані, на його думку, перебуває сусід. Маршрутизатор покладається на сусідні маршрутизатори і передає їм пакети даних тільки в тому випадку, якщо він упевнений, що вони повністю працездатні. Для з'ясування стану зв'язку маршрутизатори-сусіди досить часто обмінюються короткими повідомленнями HELLO.

Для поширення в мережі даних про стан зв'язку маршрутизатори обмінюються повідомленнями іншого типу. Ці повідомлення називаються оголошеннями про зв'язки маршрутизаторів (router links advertisement), або, точніше, про стан зв'язку. OSPF-маршрутизатори обмінюються не тільки своїми, але і чужими оголошеннями про зв'язки, одержуючи, зрештою, інформацію про стан всіх зв'язку мережі. Ця інформація і утворює граф зв'язку мережі, що, природно, той самий для всіх маршрутизаторів мережі.

Крім інформації про сусідів, маршрутизатор у своєму оголошенні перераховує IP-підмережі, з якими він зв'язаний безпосередньо, тому після одержання інформації про графа зв'язку мережі, обчислення маршруту до кожної мережі проводиться безпосередньо у цьому графі за алгоритмом Дейкстри. Більш точно, маршрутизатор обчислює шлях не до конкретної мережі, а до маршрутизатора, до якого ця мережа підключена. Кожний маршрутизатор має унікальний ідентифікатор, що передається в оголошенні про стани зв'язку. Такий підхід дає можливість не витрачати IP-адреси на зв'язку типу “точка-точка” між маршрутизаторами, до яких не підключені робочі станції [9].

Маршрутизатор обчислює оптимальний маршрут до кожної адресованої мережі, але запам'ятовує тільки перший проміжний маршрутизатор з кожного маршруту. Таким чином, результатом обчислень оптимальних маршрутів є список рядків, у яких вказується номер мережі і ідентифікатор маршрутизатора, якому потрібно переслати пакет для цієї мережі. Зазначений список маршрутів і є таблицею маршрутизації, але

обчислений він на підставі повної інформації про графа зв'язку мережі, а не часткової інформації, як у протоколі RIP.

Описаний підхід приводить до результату, що не може бути досягнутим при використанні протоколу RIP або інших дистанційно-векторних алгоритмів. RIP припускає, що всі підмережі визначеної IP-мережі мають той самий розмір, тобто, що всі вони можуть потенційно мати однакову кількість IP-вузлів, адреси яких не перекриваються. Більш того, класична реалізація RIP вимагає, щоб виділені лінії “точка-точка” мали IP-адресу, що приводить до додаткових витрат IP-адрес.

В OSPF такі вимоги відсутні: мережі можуть мати різне число хостів і можуть перекриватися. Під перекриттям розуміється наявність декількох маршрутів до однієї і тій же мережі. У цьому випадку адреса мережі в пакеті, що прийшов, може збігтися з адресою мережі, привласненим декільком портам.

Якщо адреса належить декількам підмережам у базі даних маршрутів, маршрутизатор використовує найбільш специфічний маршрут, тобто адресу підмережі, що має більш довгу маску.

Наприклад, якщо робоча група відгалужується від головної мережі, то вона має адресу головної мережі поряд з більш специфічною адресою, обумовленою маскою підмережі. При виборі маршруту до хоста в підмережі цієї робочої групи маршрутизатор знайде два шляхи, один для головної мережі і один для робочої групи. Тому що останній більш специфічний, то він і буде обраний. Цей механізм є узагальненням поняття “маршрут за замовчуванням”, використовуваного в багатьох мережах.

Використання підмереж з різною кількістю хостів є цілком природним. Наприклад, якщо в будинку або кампусі на кожному поверсі є локальні мережі, і на деяких поверхах комп'ютерів більше, ніж на інших, то адміністратор може вибрати розміри підмереж, щоб вони відображали очікувані вимоги кожного поверху, а не відповідний розмір найбільшої підмережі.

У протоколі OSPF підмережі діляться на три категорії:

- “хост-мережа” – представляє собою підмережу із однієї адреси;
- “тупикова мережа” – являє собою підмережу, підключену тільки до одного маршрутизатора;
- “транзитна мережа” – являє собою підмережу, підключену до більш, ніж одному маршрутизатору. Транзитна мережа є для протоколу OSPF

особливим випадком. У транзитній мережі декілька маршрутизаторів є взаємно та одночасно досяжними. У широко-мовних локальних мережах, таких як Ethernet або Token Ring, маршрутизатор може послати одне повідомлення, що одержать всі його сусіди. Це зменшує навантаження на маршрутизатор, коли він посиляє повідомлення для визначення існування зв'язку або оновлених оголошень про сусідів. Однак, якщо кожний маршрутизатор буде перераховувати всіх своїх сусідів у своїх оголошеннях про сусідів, то оголошення займуть багато місця в пам'яті маршрутизатора. При визначенні шляху за адресами транзитної підмережі може виявитися багато надлишкових маршрутів до різних маршрутизаторів. На обчислення, перевірку й відбраковування цих маршрутів піде багато часу.

Коли маршрутизатор починає працювати в перший раз (тобто інстальюється), він намагається синхронізувати свою базу даних з усіма маршрутизаторами транзитної локальної мережі, які за визначенням мають ідентичні бази даних. Для спрощення й оптимізації цього процесу в протоколі OSPF використовується поняття “виділеного” маршрутизатора, що виконує дві функції.

По-перше, виділений маршрутизатор і його резервний “напарник” є єдиними маршрутизаторами, з якими новий маршрутизатор буде синхронізувати свою базу. Синхронізувавши базу з виділеним маршрутизатором, новий маршрутизатор буде синхронізований з усіма маршрутизаторами даної локальної мережі.

По-друге, виділений маршрутизатор оголошує про мережні зв'язки, перераховуючи своїх сусідів підмережі. Інші маршрутизатори просто повідомляють про свій зв'язок з виділеним маршрутизатором.

Це робить оголошення про зв'язки (яких багато) більш короткими, розміром з оголошення про зв'язки окремої мережі. Для початку роботи маршрутизатора OSPF потрібен мінімум інформації – IP-конфігурація (IP-адреси і маски підмереж), деяка інформація за замовчанням (default) і команда на включення. Для багатьох мереж інформація за замовчанням досить схожа. У той же час протокол OSPF передбачає високий ступінь програмування.

Інтерфейс OSPF (порт маршрутизатора, що підтримує протокол OSPF) є узагальненням підмережі IP. Подібно підмережі IP, інтерфейс OSPF має IP-адресу і маску підмережі. Якщо один порт OSPF підтримує більш ніж одну підмережу, протокол OSPF розглядає ці підмережі так, ніби вони були на різних фізичних інтерфейсах, і обчислює маршрути відповідно.

Інтерфейси, до яких підключені локальні мережі, називаються ширококомовними (broadcast) інтерфейсами, тому що вони можуть використовувати ширококомовні можливості локальних мереж для обміну сигнальною інформацією між маршрутизаторами. Інтерфейси, до яких підключені глобальні мережі, що не підтримують ширококомовлення, але забезпечуючі доступ до багатьох вузлів через одну точку входу, наприклад мережі X.25 або frame relay, називаються неширокомовними інтерфейсами із множинним доступом або NBMA (non-broadcast multi-access). Вони розглядаються аналогічно ширококомовним інтерфейсам за винятком того, що ширококомовне розсилання емулюється шляхом посилки повідомлення кожному сусіду. Тому що виявлення сусідів не є автоматичним, як у ширококомовних мережах, NBMA-сусіди повинні задаватися при конфігуруванні вручну. Як на ширококомовних, так і на NBMA-інтерфейсах можуть бути задані пріоритети маршрутизаторів для того, щоб вони могли вибрати виділений маршрутизатор.

Інтерфейси “точка-точка”, подібні PPP, трохи відрізняються від традиційної IP-моделі. Хоча вони і можуть мати IP-адреси і підмаску, але необхідності в цьому немає.

В простих мережах досить визначити, що пункт призначення досяжний і знайти маршрут, що буде задовільним. В складених мережах звичайно є декілька можливих маршрутів. Іноді хотілося б мати можливості щодо встановлення додаткових критеріїв для вибору шляху: наприклад, найменша затримка, максимальна пропускна здатність або найменша вартість (в мережах з оплатою за пакет). Із цих причин протокол OSPF дозволяє мережному адміністратору призначати кожному інтерфейсу визначену кількість, названу *метрикою*, щоб вплинути на вибір маршруту. Число, використовуємо як метрика шляху, може бути призначено довільним образом за бажанням адміністратора. Але за замовчуванням як метрика використовується час передачі біта в 10-ти наносекундних одиницях (10 Мб/с Ethernet призначається значення 10, а лінії 56 Кб/с – кількість 1785). *Метрика шляху*, що обчислюється протоколом OSPF, являє собою суму метрик всіх прохідних у шляху зв'язку; це дуже груба оцінка затримки шляхів. Якщо маршрутизатор виявляє більш, ніж один шлях до вилученої підмережі, то він використовує шлях з найменшою вартістю шляху.

У протоколі OSPF використовується декілька часових параметрів, і серед них найбільш важливими є інтервал повідомлення HELLO і інтервал відмови маршрутизатора (router dead interval). HELLO – це повідомлення,

яким обмінюються сусідні, тобто безпосередньо зв'язані маршрутизатори підмережі, з метою встановити стан лінії зв'язку і стан маршрутизатора-сусіда. У повідомленні HELLO маршрутизатор передає свої робочі параметри і говорить про те, кого він розглядає своїми найближчими сусідами. Маршрутизатори з різними робочими параметрами ігнорують повідомлення HELLO один одного, тому невірні сконфігуровані маршрутизатори не будуть впливати на роботу мережі. Кожний маршрутизатор шле повідомлення HELLO кожному своєму сусідові, принаймні, один раз протягом інтервалу HELLO. Якщо інтервал відмови маршрутизатора минає без одержання повідомлення HELLO від сусіда, то вважається, що сусід непрацездатний, і поширюється нове оголошення про мережні зв'язки, щоб в мережі відбувся перерахунок маршрутів.

7.2. Стек IPX/SPX

7.2.1. Загальна характеристика протоколу IPX

Цей стек є оригінальним стеком протоколів фірми Novell, що вона розробила для своєї мережної операційної системи NetWare ще на початку 80-х років. Протоколи Internetwork Packet Exchange (IPX) і Sequenced Packet Exchange (SPX), які дали ім'я стеку, є прямою адаптацією протоколів XNS фірми Херох, розповсюджених у набагато меншій ступені, ніж IPX/SPX. За кількістю установок протоколи IPX/SPX лідирують, і це обумовлено тим, що сама ОС NetWare займає лідируюче положення із долі установок у світовому масштабі приблизно в 65%. Сімейство протоколів фірми Novell і відповідність моделі ISO/OSI наведено на рис. 7.8.

На *фізичному та канальному рівнях* в мережах Novell використовуються всі популярні протоколи цих рівнів (Ethernet, Token Ring, FDDI і інші).

На *мережному рівні* у стеку Novell працює *протокол IPX*, а також протоколи обміну маршрутною інформацією *RIP* і *NLSP* (аналог протоколу OSPF стека TCP/IP). IPX є протоколом, що займається питаннями адресації й маршрутизації пакетів в мережах Novell. Маршрутні рішення IPX засновані на адресних полях у заголовку його пакета, а також на інформації, що надходить від протоколів обміну маршрутною інформацією. Наприклад, IPX використовує інформацію, що поставляється або протоколом RIP, або протоколом NLSP (NetWare Link State Protocol) для передачі пакетів комп'ютеру призначення або наступному маршрутизатору. Протокол IPX

підтримує тільки дейтаграмний спосіб обміну повідомленнями, за рахунок чого ощадливо споживає обчислювальні ресурси. Отже, протокол IPX забезпечує виконання трьох функцій: завдання адреси, встановлення маршруту та розсилання дейтаграм.

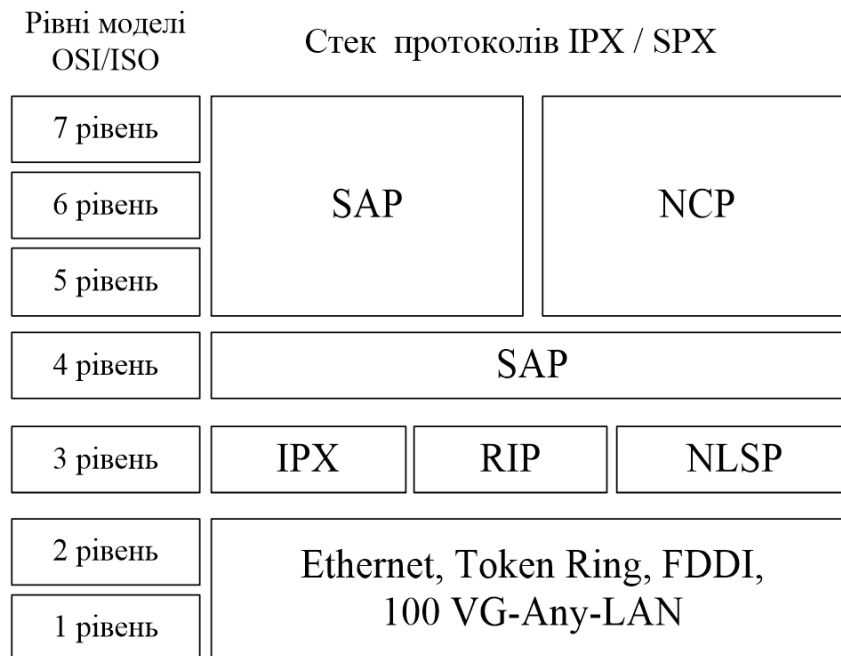


Рис. 7.8. Стек IPX / SPX

На транспортному рівні моделі OSI у стеку Novell відповідає протокол SPX, що здійснює передачу повідомлень із встановленням з'єднань.

На верхніх прикладному, представницькому та сеансовому рівнях працюють протоколи NCP і SAP. Протокол NCP (NetWare Core Protocol) є протоколом взаємодії сервера NetWare і оболонки робочої станції. Цей протокол прикладного рівня реалізує архітектуру клієнт-сервер на верхніх рівнях моделі OSI. За допомогою функцій цього протоколу робоча станція робить підключення до сервера, відображає каталоги сервера на локальні букви дисководів, переглядає файлову систему сервера, копіює вилучені файли, змінює їхні атрибути та інше., а також здійснює поділ мережного принтера між робочими станціями.

SAP (Service Advertising Protocol) – протокол оголошення про сервіс – концептуально подібний до протоколу RIP. Подібно тому, як протокол RIP дозволяє маршрутизаторам обмінюватися маршрутною інформацією, протокол SAP дає можливість мережним пристроям обмінюватися інформацією про наявні мережні сервіси.

Сервери й маршрутизатори використовують SAP для оголошення про свої сервісні послуги та мережні адреси. Протокол SAP дозволяє мережним

пристроєм постійно коректувати дані про те, які сервісні послуги є зараз у мережі. При старті сервери використовують SAP для оповіщення частини мережі, що залишилася, про свої послуги. Коли сервер завершує роботу, то він використовує SAP для того, щоб сповістити мережу про припинення дії своїх послуг.

В мережах Novell сервери NetWare 3.x щохвилини розсилають широкомовні пакети SAP. Пакети SAP у значній мірі засмічують мережу, тому однієї з основних задач маршрутизаторів, що виходять на глобальні зв'язки, є фільтрація трафіку SAP-пакетів і RIP-пакетів.

Особливості стека IPX/SPX обумовлені особливостями ОС NetWare, а саме орієнтацією її ранніх версій (до 4.0) на роботу в локальних мережах невеликих розмірів, що складаються з персональних комп'ютерів зі скромними ресурсами. Тому Novell потрібні були протоколи, на реалізацію яких була потрібна мінімальна кількість оперативної пам'яті (обмеженої в IBM-сумісних комп'ютерах під управлінням MS-DOS 640 Кбайтами) і які б швидко працювали на процесорах невеликої обчислювальної потужності. У результаті, протоколи стека IPX/SPX донедавна добре працювали в локальних мережах і не дуже – у великих корпоративних мережах, тому що занадто перевантажували повільні глобальні зв'язки широкомовними пакетами, які інтенсивно використовуються декількома протоколами цього стека (наприклад, для встановлення зв'язку між клієнтами та серверами).

Ця обставина, а також той факт, що стік IPX/SPX є власністю фірми Novell і на його реалізацію потрібно одержувати в неї ліцензію, довгий час обмежували поширеність його тільки мережами NetWare. Однак до моменту випуску версії NetWare 4.0, Novell внесла й продовжує вносити у свої протоколи серйозні зміни, спрямовані на пристосування їх для роботи в корпоративних мережах. Зараз стік IPX/SPX реалізований не тільки в NetWare, але і у декількох інших популярних мережних ОС – SCO UNIX, Sun Solaris, Microsoft Windows NT [17; 26].

7.2.2. Формат пакету IPX

Пакет протоколу IPX має набагато більш просту структуру в порівнянні з пакетом IP, що, власне, і відбиває менші функціональні можливості протоколу IPX [7; 17].

IPX-пакет має поля, наведені в табл. 7.7.

Контрольна сума (Checksum) – це 2-байтове поле, що є “пережитком минулого”, що протокол IPX веде ще від протоколу IDP стека Xerox. Тому що низькорівневі протоколи (наприклад, Ethernet) завжди виконують

перевірку контрольних сум, але IPX не використовує це поле і завжди встановлює його в одиниці.

Таблиця 7.7.

Поля заголовку IPX пакету

Поле заголовку	Довжина в байтах
Checksum-контрольна сума	2
Length-загальна довжина пакету	2
TransportControl-лічильник пройдених мостів	1
PacketType тип пакету	1
DestNetwork-адреса мережі отримувача	4
DestNode-адреса станції отримувача	6
DestSocet-сокет програми-отримувача	2
SourceNetwork-адреса мережі отримувача	4
SourceNode-адреса вузла відправника	6
SourceSocet-сокет програми-відправника	2
DATA-данні	0 – 564

Довжина (Length) займає 2 байти і задає розмір усього пакета, включаючи IPX-заголовок і поле даних. Самий короткий пакет - 30 байт - включає тільки IPX-заголовок, а рекомендований максимально великий - 576 байт - включає IPX-заголовок плюс 546 байт даних. Максимальний розмір пакета в 576 байт відповідає рекомендаціям стандартів Internet для складених мереж. Протокол IPX обчислює значення, ґрунтуючись на інформації, наданою прикладною програмою при виклику функції IPX. IPX-пакет може перевершувати максимум, що рекомендується, у 576 байт, що і відбувається в локальних мережах Ethernet, де використовуються IPX-пакети в 1500 байт із полем даних у 1470 байт.

Керування транспортом (Transport control) має довжину 8 біт. Це поле визначає час життя пакета. IPX-пакет може перетнути до 15 маршрутизаторів. Протокол IPX встановлює це одnobайтове поле в 0 до початку передачі, а потім збільшує його на 1 щораз, коли пакет проходить через маршрутизатор. Якщо лічильник перевищить 15, то пакет анулюється.

Тип пакета (Packet type) має довжину 8 біт. Фірма Херох визначила у свій час визначені значення для різних типів пакетів: прикладні програми, що

посилають IPX-пакети, повинні встановлювати це поле в значення, рівне 4. Значення 5 відповідає службовим IPX-пакетам, використовуваним протоколом SPX як службові повідомлення. Значення 17 указує на те, що в поле даних IPX-пакета знаходиться повідомлення протоколу NetWare Core Protocol (NCP) - основного протоколу файлової служби NetWare.

Адреса призначення (Destination address) - складається з трьох полів: номера мережі призначення, номера вузла призначення, номера сокету призначення. Ці поля займають відповідно 4, 6 і 2 байти.

Адреса відправника (Source address) – номер вихідної мережі, номер вихідного вузла, номер вихідного сокету. Аналогічні адресним полям призначення.

Поле даних (Data). Може займати від 0 до 546 байт. Поле даних нульової довжини може використовуватися в службових пакетах, наприклад, для підтвердження одержання попереднього пакета. З аналізу формату пакета можна зробити деякі висновки про обмеження протоколу IPX.

Відсутня можливість динамічної фрагментації на мережному рівні. У IPX-пакеті немає полів, за допомогою яких маршрутизатор може розбити занадто великий пакет на частини. При передачі пакета в мережу з меншим значенням MTU IPX-маршрутизатор відкидає пакет. Протокол верхнього рівня, наприклад NCP, повинний послідовно зменшувати розмір пакета доти, поки не одержить на нього позитивну квитанцію.

Великі накладні витрати на службову інформацію. Порівняно невелика максимальна довжина поля даних IPX-пакета (546 байт при довжині заголовка 30 байт) приводить до того, що як мінімум 5 % даних є службовими.

Час життя пакета обмежено числом 15, що може виявитися недостатнім для великої мережі (для порівняння, у IP-мережах пакет може пройти до 255 проміжних маршрутизаторів).

Відсутнє поле якості сервісу, що не дозволяє маршрутизаторам автоматично налаштовуватися до вимог додатка якості передачі трафіку.

Крім того, деякі недоліки мереж Novell пов'язані не з протоколом IPX, а із властивостями інших протоколів стека IPX/SPX. Багато недоліків виявляються при роботі стека IPX/SPX на повільних глобальних лініях зв'язку, і це закономірно, тому що ОС NetWare оптимізувалась для роботи в локальній мережі.

Наприклад, неефективна робота по відбудові загублених і викривлених пакетів з помилкою на низько швидкісних глобальних каналах обумовлена

тим, що протокол NCP, що виконує цю роботу, використовує метод одержання квитанцій із простоями. У локальних мережах зі швидкістю 10 Мбіт/с такий метод працював цілком ефективно, а на повільних каналах час чекання квитанції помітно гальмує роботу вузла, який передає.

У версіях ОС NetWare до 4.0 відповідність символічних імен серверів їх мережним адресам встановлювалося тільки за допомогою широкомовного протоколу Service Advertising Protocol (SAP). Однак широкомовні розсилання помітно засмічують повільні глобальні канали. Модернізуючи свій стек для застосування у великих корпоративних мережах, компанія Novell використовує тепер довідкову службу NDS (NetWare Directory Services) для перебування різноманітної інформації про наявних в мережі ресурсах і службах, у тому числі і про відповідність імені сервера його мережній адресі. Тому що служба NDS підтримується тільки серверами з версією NetWare 4.x і вище, тому для роботи з версіями NetWare 3.x маршрутизатори розпізнають SAP-пакети за номером їх сокета і передають їх на всі порти, імітуючи широкомовні розсилання локальної мережі, на що витрачається значна частина пропускну здатності повільних глобальних ліній. Крім того, така “псевдо ширококорозповсюджуваність” зводить нанівець ізоляцію мереж від некоректних SAP-пакетів.

В останніх версіях своєї операційної системи NetWare компанія Novell значно модифікувала свій стек для того, щоб він міг більш ефективно використовуватися у великих складених мережах [7].

Служба NDS дозволяє відмовитися від широкомовного протоколу SAP. Служба NDS заснована на ієрархічній розподіленій базі даних, що зберігає інформацію про користувачів і поділювані ресурси мережі. Додатки звертаються до цієї служби за протоколом прикладного рівня NDS.

Додано модуль для реалізації методу ковзного вікна – що має назву Burst Mode Protocol NLM.

Додано модуль для підтримки довгих IPX-пакетів у глобальних мережах - Large Internet Packet NLM.

Крім того, постійне підвищення швидкодії глобальних служб зменшує недоліки оригінальних протоколів стека IPX/SPX, що дозволяє деяким оглядачам говорити про успішну роботу операційної системи NetWare у глобальних мережах і без зазначених нововведень.

7.2.3. Маршрутизація протоколу IPX

У цілому маршрутизація протоколу IPX виконується аналогічно маршрутизації протоколу IP. Кожен IPX-маршрутизатор підтримує таблицю маршрутизації, на підставі якої приймається рішення про просування пакета. IPX-маршрутизатори підтримують однокрокову маршрутизацію, при якій кожен маршрутизатор приймає рішення тільки про вибір наступного на шляху маршрутизатора. Можливості маршрутизації від джерела в протоколі IPX відсутні.

У полі “Номер мережі” вказується шістнадцятирічна адреса мережі призначення, а в полі “Наступний маршрутизатор” – повна мережна адреса наступного маршрутизатора, тобто пари “номер мережі – MAC-адреса”. MAC-адреса з цього запису переноситься в поле адреси призначення кадру канального рівня, наприклад Ethernet, що і переносить IPX-пакет наступному маршрутизатору. IPX-пакет при передачі між проміжними маршрутизаторами змін не перетерплює.

Якщо IPX-маршрутизатор виявляє, що мережа призначення - це його безпосередньо підключена мережа, то з заголовка IPX-пакета витягається номер вузла призначення, що є MAC - адресою вузла призначення. Ця MAC-адреса переноситься на адресу призначення кадру канального рівня, наприклад FDDI. Кадр безпосередньо відправляється в мережу, і протокол FDDI доставляє його за цією адресою вузлу призначення.

IPX-маршрутизатори звичайно використовують два типи метрики при виборі маршруту: відстань і затримку в деяких умовних одиницях – тиках (ticks). Відстань у хопх має звичайний сенс – це кількість проміжних маршрутизаторів, які потрібно перетнути IPX-пакету для досягнення мережі призначення. Затримка також часто використовується в маршрутизаторах і мостах/комутаторах для більш точного порівняння маршрутів. Однак у IPX-маршрутизаторах традиційно затримка вимірюється в тиках таймера персонального комп’ютера, що видає сигнал переривання 18,21 рази в секунду. Ця традиція ведеться від перших програмних IPX-маршрутизаторів, що працювали в складі операційної системи NetWare і користувалися таймером персонального комп’ютера для виміру інтервалів часу. Нагадаємо, що IP-маршрутизатори, а також мости/комутатори, що підтримують протокол Spanning Tree, вимірюють затримку, внесену якою-небудь мережею в 10-наносекундних одиницях передачі одного біта інформації, так що мережа Ethernet оцінюється затримкою в 10 одиниць. Крім цього, IPX-

маршрутизатори оцінюють затримку не одного біта, а стандартного для IPX-пакета в 576 байт.

Тому затримка в тиках для мережі Ethernet дорівнює 0,00839 тика, а для каналу 64 Кбіт/с – 1,31 тика. Затримка в тиках завжди округляється до цілого числа тиків у велику сторону, так що мережа Ethernet вносить затримку в один тик, а канал 64 Кбіт/с – у 2 тики. При обчисленні метрики в тиках для складеного маршруту затримки в тиках складаються.

Дві метрики в записах таблиці маршрутизації протоколу IPX використовуються в порядку пріоритетів. Найбільшим пріоритетом володіє метрика, обмірювана в затримках, а якщо ця метрика збігається для яких-небудь маршрутів, то в увагу приймається відстань у хопх.

Незважаючи на традиції виміру затримки в тиках, IPX-маршрутизатори можуть використовувати і стандартні затримки мереж, обмірювані в 10-наносекундних інтервалах.

IPX-маршрутизатори можуть підтримувати як статичні маршрути, так і динамічні, отримані за допомогою протоколів RIP IPX і NLSP.

Протокол RIP IPX дуже близький до протоколу RIP IP. Тому що в IPX-мережах маски не застосовуються, тому RIP IPX не має аналога RIPv2, що передає маски. Інтервал між оголошеннями в протоколу RIP IPX дорівнює 60 с (на відміну від 30 RIP IP). У пакетах RIP IPX для кожної мережі вказуються обидві метрики – у тиках. Для виключення маршрутних петель IPX-маршрутизатори використовують прийом розщеплення обрію.

Час життя динамічного запису складає 180 с. Недосяжність мережі вказується значенням числа хопів у 15 (0x), а тиків - у 0xFFFF.

IPX-маршрутизатори, як і IP-маршрутизатори, не передають з мережі в мережу пакети, що мають широкомовну мережну адресу. Однак для деяких типів таких пакетів IPX-маршрутизатори роблять виключення. Це пакети служби SAP, за допомогою якої сервери NetWare повідомляють про себе по мережі. IPX-маршрутизатори передають SAP-пакети в усі безпосередньо підключені мережі, крім тієї, від якої цей пакет отриманий (розщеплення обрію). Якби IPX-маршрутизатори не виконували таких передач, то клієнти NetWare не змогли б взаємодіяти із серверами в мережі, розділеній маршрутизаторами, у звичному стилі, тобто шляхом перегляду наявних серверів за допомогою команди SLIST.

IPX-маршрутизатори завжди використовують внутрішній номер мережі, що відноситься не до інтерфейсів маршрутизатора, а до самого модуля маршрутизації. Внутрішній номер мережі є деяким аналогом мережі

127.0.0.0 вузлів IP-мереж, однак кожен IPX-маршрутизатор повинен мати унікальний внутрішній номер мережі, причому його унікальність повинна поширюватися і на зовнішні номери IPX-мереж у складній мережі.

IPX-маршрутизатори виконують також функцію узгодження форматів кадрів Ethernet. У складних IPX-мережах кожна мережа може працювати тільки з одним з 4-х можливих типів кадрів IPX. Тому якщо в різних мережах використовуються різні типи кадрів Ethernet, то маршрутизатор посилає в кожную мережу той тип кадру, що встановлений для цієї мережі.

Протокол NLSP (NetWare Link Services Protocol) являє собою реалізацію алгоритму стану зв'язку для IPX-мереж. В основному він працює аналогічно протоколу OSPF мереж TCP/IP.

7.3. Стек NetBIOS/SMB

Фірми Microsoft і IBM спільно працювали над мережними засобами для персональних комп'ютерів, тому стек протоколів NetBIOS/SMB є їх спільним дітищем. Засоби NetBIOS з'явилися в 1984 році як мережне розширення стандартних функцій базової системи введення/виводу (BIOS) IBM PC для мережної програми PC Network фірми IBM, що на прикладному рівні (рис. 7.9) використовувала для реалізації мережних сервісів протокол SMB (Server Message Block).

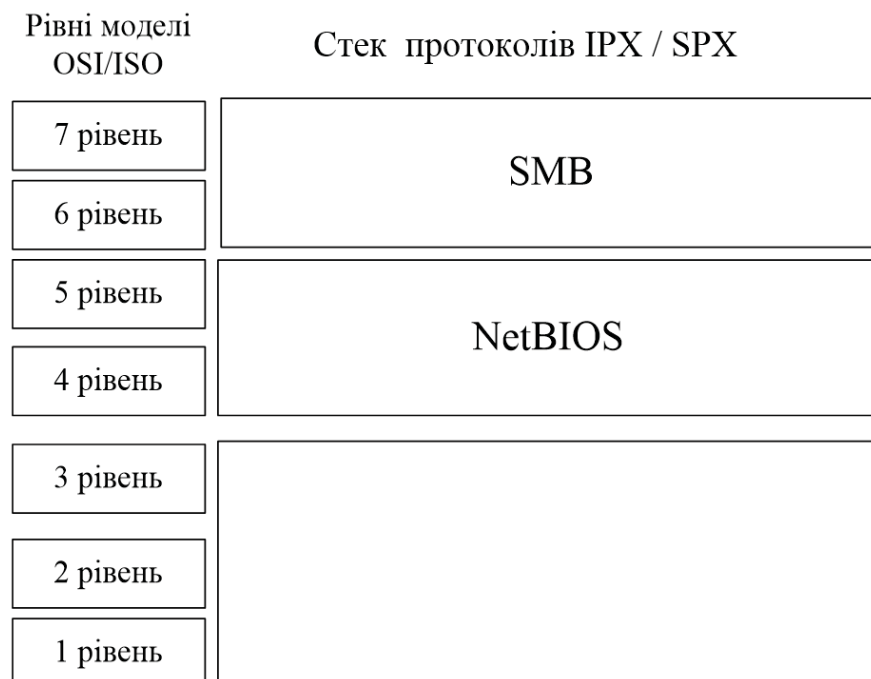


Рис. 7.9. Стік NetBIOS / SMB

Протокол NetBIOS працює на трьох рівнях моделі взаємодії відкритих систем: мережному, транспортному та сеансовому. NetBIOS може забезпечити сервіс більш високого рівня, ніж протоколи IPX і SPX, однак не має здатність до маршрутизації.

Таким чином, NetBIOS не є мережним протоколом у точному значенні цього слова. NetBIOS містить багато корисних мережних функцій, які можна віднести до мережного, транспортному та сеансовому рівнів, однак з його допомогою неможлива маршрутизація пакетів, тому що в протоколі обміну кадрами NetBIOS не вводиться таке поняття як мережа. Це обмежує застосування протоколу NetBIOS локальними мережами, не розділеними на підмережі. NetBIOS підтримує як дейтаграмний обмін, так і обмін із встановленням з'єднань.

Протокол SMB, що відповідає прикладному та представницькому рівням моделі OSI, регламентує взаємодію робочої станції із сервером. У функції SMB входять наступні операції:

Управління сесіями. Створення та розрив логічного каналу між робочою станцією та мережними ресурсами файлового сервера.

Файловий доступ. Робоча станція може звернутися до файл-серверу із запитом на створення та видалення каталогів, створення, відкриття та закриття файлів, читання і запис у файли, перейменування й видалення файлів, пошук файлів, одержання й установку файлових атрибутів, блокування записів.

Сервіс друку. Робоча станція може ставити файли в чергу для друку на сервері і одержувати інформацію про чергу друку.

Сервіс повідомлень. SMB підтримує просту передачу повідомлень із наступними функціями: надіслати просте повідомлення; надіслати широкомовне повідомлення; послати початок блоку повідомлень; надіслати текст блоку повідомлень; послати кінець блоку повідомлень; переслати ім'я користувача; скасувати пересилання; одержати ім'я машини.

Через велику кількість програм, які використовують функції API, призначені NetBIOS, у багатьох мережних ОС ці функції реалізовані у вигляді інтерфейсу до своїх транспортних протоколів. В NetWare є програма, що емулює функції NetBIOS на основі протоколу IPX, існують програмні емулятори NetBIOS для Windows NT і стека TCP/IP [3;17; 26; 43].

7.4. Протоколи архітектури Apple Talk

Apple Talk була розроблена як система розподіленої мережі клієнт-сервер. Інакше кажучи, користувачі спільно користуються мережними ресурсами (такими, як файли і принтери). Комп'ютери, що забезпечують ці ресурси, називаються серверами (servers); комп'ютери, що використовують мережні ресурси службових пристроїв, називаються клієнтами (clients). Взаємодія зі службовими пристроями в значній мірі є прозорою для користувача, тому що сам комп'ютер визначає місце розташування запитуваного матеріалу та звертається до нього без одержання подальшої інформації від користувача. На додаток до простоти використання, розподілені системи також мають економічні переваги в порівнянні із системами, де всі рівні, тому що важливі матеріали можуть бути поміщені в декількох, а не в багатьох місцях розташування.

Apple Talk відносно добре погодиться з еталонною моделлю OSI. На рис. 7.10 “*Apple Talk* і еталонна модель OSI” наведені протоколи *Apple Talk*, суміжні з тими рівнями OSI, з якими в них встановлена відповідність.

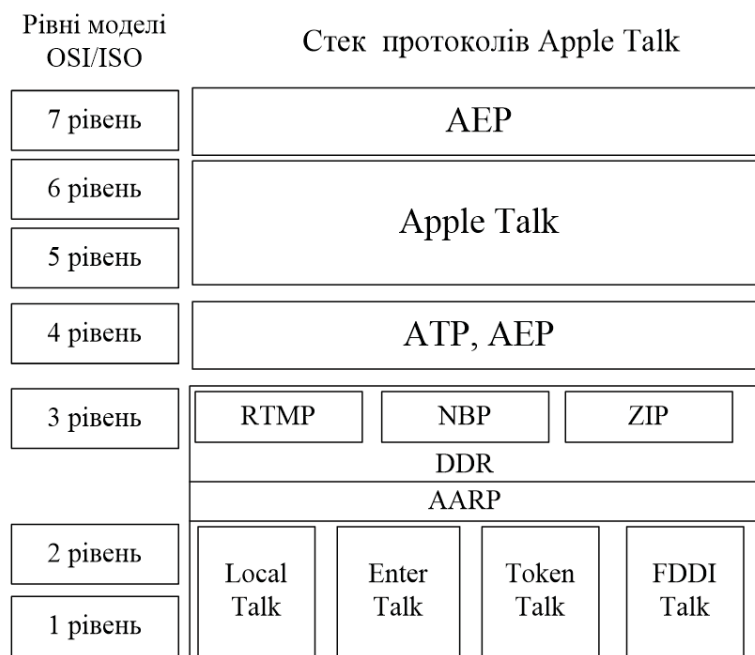


Рис. 7.10. *Apple Talk* і еталонна модель OSI

Цей рисунок відрізняється від інших зображень зв'язку пакета протоколів *Apple Talk* з моделлю OSI тим, що на ньому NBP, ZIP і RTMP розміщені на рівні 3, а AEP – на рівні 7. На думку Cisco, NBP, ZIP і RTM за

своїми функціональними можливостями стоять ближче до рівня 3 моделі OSI, хоча вони і користуються послугами DDP, іншого протоколу рівня 3. Аналогічно, Cisco думає, що API варто включити в перелік протоколів прикладного рівня, тому що він звичайно використовується для забезпечення функціональних можливостей прикладного рівня. Зокрема, AEP допомагає визначити можливість віддалених вузлів приймати наступні з'єднання.

Короткий опис протоколів наведений у табл. 7.8.

Таблиця 7.8.

Опис протоколів

№ п/п	Позначення	Назва протоколу	Призначення протоколу
1	AURP	Apple Talk Update-based Routing Protocol	Протокол маршрутизації
2	RTMP	Routing Table Maintenance Protocol	Протокол обміну маршрутною інформацією
3	AEP	Apple Talk Echo Protocol	Протокол перевірки доступності об'єктів
4	ATP	Apple Talk Transaction Protocol	Транспортний протокол, орієнтований на з'єднання
5	NBR	Name Binding Protocol	Протокол прив'язки імен до мережних адрес
6	DDP	Datagram Delivery Protocol	Протокол мережного рівня
8	AARP	Apple Talk Address Resolution Protocol	Протокол прив'язки адреси мережної карти до мережної адреси
10	ASP	Apple Talk Session Protocol	Протокол сеансового рівня
12	PAP	Printer Access Protocol	Протокол доступу до принтерів
13	ADSP	Apple Talk Data Stream Protocol	Протокол потоку даних

7.5. Мережна архітектура NetWare

Як середовище NOS, NetWare визначає п'ять вищих рівнів еталонної моделі OSI. Вона забезпечує спільне користування файлами й принтером, підтримку різних прикладних задач, таких як передача електронної пошти та доступ до бази даних, і інші послуги. Також, як і інші NOS, такі як *Network File*

System (NFS) компанії Sun Microsystems, Inc. і *LAN Manager* компанії Microsoft Corporation, NetWare базується на архітектурі клієнт-сервер (*client-server architecture*). У таких архітектурах клієнти (робочі станції) запитують у серверів визначені послуги, такі як доступ до файлів і принтера.

Спочатку клієнтами NetWare були невеликі PC, у той час як серверами були ненабагато потужніші PC. Після того, як NetWare стала більш популярною, вона була перенесена на інші комп'ютерні платформи. У наш час клієнти і сервера можуть бути представлені практично будь-яким видом комп'ютерної системи.

Основна характеристика системи клієнт-сервер полягає в тому, що доступ до віддаленої мережі є прозорим для користувача. Це досягається за допомогою віддаленого виклику процедур (*remote procedure calls*) – такого процесу, коли програма місцевого комп'ютера, що працює на встаткуванні клієнта, відправляє виклик у віддалений сервер. Цей сервер виконує зазначену процедуру та повертає запитану інформацію клієнту місцевого комп'ютера. Рис. 7.11 ілюструє в спрощеному виді відомі протоколи NetWare та їх зв'язок з еталонною моделлю OSI.

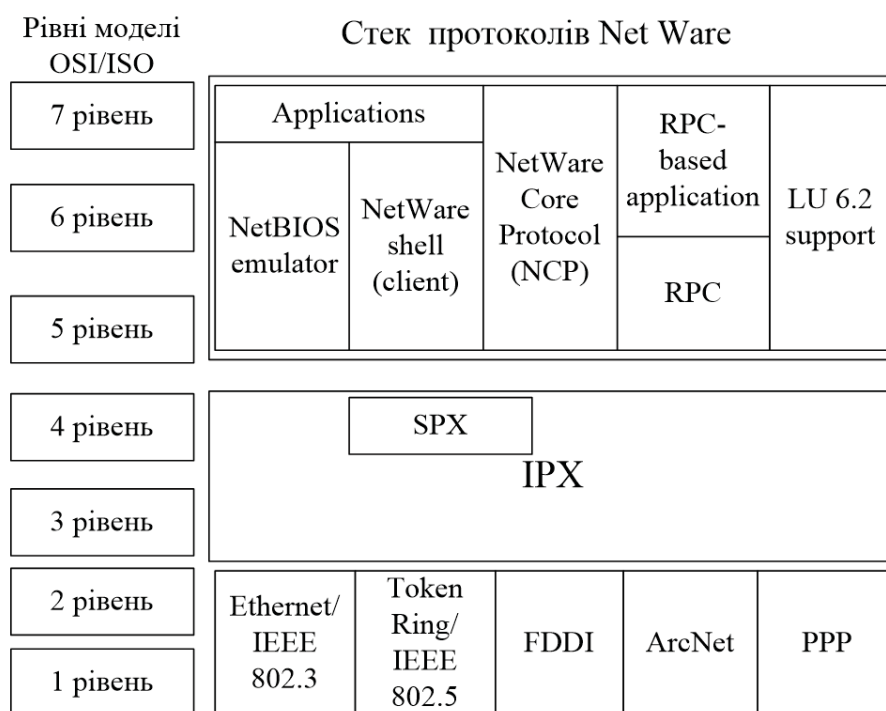


Рис. 7.11. Протоколи NetWare та їх зв'язок з моделлю OSI

При наявності відповідних драйверів, NetWare може працювати з будь-яким протоколом доступу до носія. На рисунку перераховані ті протоколи доступу до носія, які в наш час забезпечуються драйверами NetWare.

7.6. Протоколи архітектури SNA (фірми IBM)

Логічна архітектура SNA складається із шести рівнів. Три верхніх рівні (служби управління функціями, управління потоком даних, управління передачею) забезпечують організацію й обслуговування сесій при обміні даними, три нижніх рівні (управління шляхами, управління ланкою даних, фізичний) – маршрутизацію й фізичну передачу даних. Для обміну інформацією в SNA використовується набір протоколів зв'язку між еквівалентними рівнями. Однорідні рівні взаємодіють шляхом обміну параметрами, що містяться в заголовках.

Кожний мережний ресурс або вузол в SNA називається адресованим елементом мережі (NAU) і має відповідну мережну адресу, за якою здійснюється маршрутизація між NAU. Передбачено два типи NAU: фізичні елементи (PU) і логічні елементи (LU). Є 4 типи PU: типу 1, реалізований у терміналах, випущених до введення SNA; типу 2, реалізований у концентраторах, подібних IBM 3274; типу 3 – відсутній; типу 4, реалізований у зв'язних процесорах; типу 5, реалізований в VTAM.

Особливості протоколів архітектури SNA полягають у наступному. Основною функцією рівня управління ланкою даних є забезпечення безпомилкової передачі кадрів, для чого організується повторна передача кадрів з помилкою. Як основний протокол ланки передачі даних використовується протокол SDLC, можуть підтримуватися й інші протоколи, включаючи BSC, асинхронні стартостопні процедури й протокол X.25.

Типова структура кадру SNA наведена на рис. 7.12

Типова структура кадру SNA				
Заголовок	Заголовок	Заголовок	Дані	Кінцевик
SDLC	TH (протокол PC)	RH (протокол TC)		SDLC
		< BIO >		
	< BTU >			
BIO – базовий інформаційний елемент; BTU – базовий елемент передачі.				

Рис. 7.12. Типова структура кадру SNA

BTU – базовий елемент передачі, є основним транспортним елементом архітектури. BTU крім SDLC може бути переданий і іншими протоколами,

наприклад Frame Relay, Ethernet, X.25, X.75, IP, TCP і ін. На рівні управління шляхами (протокол PC) формується заголовок TH який має декілька форматів, описаних нижче.

На рівні управління передачею (протокол TC) формується заголовок RH, що містить сукупність параметрів управління передачею (темپ обміну, індикатори зчеплення, режимів і ін.).

Рівень управління потоком даних (протокол DFC) підтримує потік і логічне формування даних між кінцевими користувачами за допомогою методів зчеплення (виводу в дужки) і формування режимів запитів/відповідей. Дужки – це послідовність запитів і відповідей, які становлять цикл обміну. Відповідні параметри містяться в заголовки RH. Абоненти мережі SNA через шлюзи мережного рівня (протокол PC) можуть взаємодіяти з абонентами мереж TCP/IP, ISO і навпаки [17; 43].

7.7. Мережна архітектура DNA

На противагу існуючій думці, DECnet зовсім не є архітектурою мережі, а являє собою ряд виробів, що відповідає архітектурі цифрової мережі (Digital Network Architecture – DNA) компанії Digital. Як і більшість інших складних мережних архітектур, що поставляються великими постачальниками систем, DNA підтримує великий набір як патентованих, так і стандартних протоколів. Перелік технологій, які підтримує DNA, постійно росте в міру того, як Digital реалізує нові протоколи. Рис. 7.13 ілюструє неповну картину DNA і зв'язок деяких її компонентів з еталонною моделлю OSI.

Основним комутаційним елементом мережної архітектури DNA є вузол. Всі вузли рівноправні, тобто кожний вузол, може виступати як будь-який функціональний елемент інформаційно-обчислювальної системи (ІОС). Вузли закріплені за різними областями. Кожна область має свого адміністратора та засоби маршрутизації. Кожний вузол має свою унікальну адресу. Структура адреси DECnet-4: 1 байт – номер області, 1 байт – номер підобласті, 6 байт – Ethernet адреса.

Так як мережі DECnet є частками, кожний власник такої мережі вправі відмовитися від яких-небудь протоколів DECnet і реалізувати інші, що забезпечують послуги та міжмережні інтерфейси, необхідні суміжним рівням. Наприклад, використовуються протоколи DDCMP, Ethernet, DNA, NSP, DAP, NICE, SMB і ін. Перелік протоколів використовуваних архітектурою наведений у табл. 7.9.

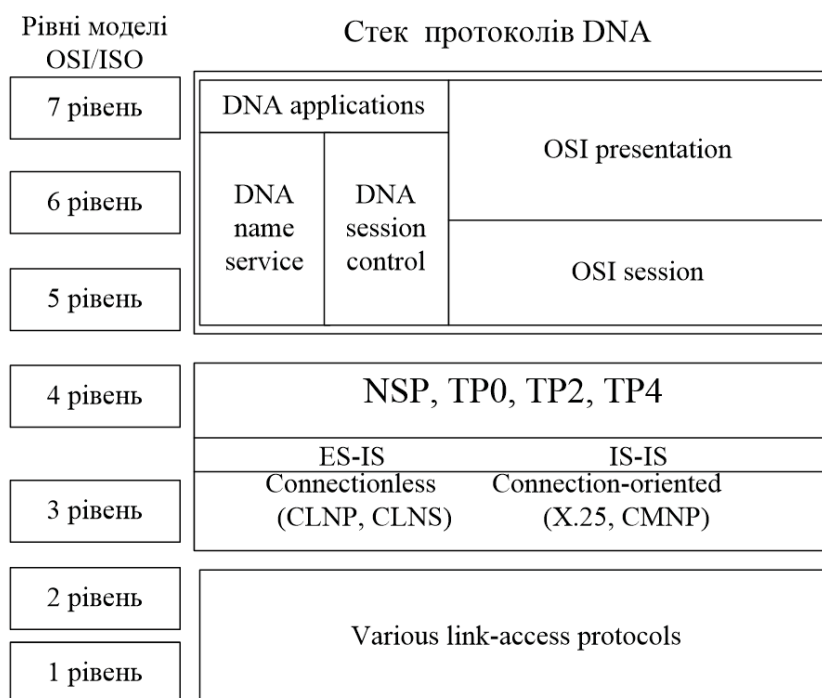


Рис. 7.13. DNA і еталонна модель OSI

Таблиця 7.9.

Перелік протоколів використовуваних архітектурою

Позначення	Назва протоколу (анг.)	Призначення протоколу
DRP	DECnet Routing Protocol	Протокол маршрутизації та комутації пакетів
NSP	Network Services Protocol DNA	Протокол мережної служби
SSP	Network Information and Command Exchange Protocol	Протокол обміну мережною інформацією управління
DAP	Data Access Protocol	Протокол доступу до даних
CNTRM	Network Command Terminal	Протокол мережного командного термінала
MOP	Maintenance Operations Protocol	Протокол технічного обслуговування
LAT	Local Area Transport Protocol	Транспортний протокол локальної області
DNS	Distributed Name Server	Розподілений сервер імен
SCP	Session Control Protocol DNA	Протокол управління сеансом DNA
FOUND	Foundation Services	Протокол управління основними сервісними процедурами
SCP	Session Control Protocol	Протокол управління сеансом

7.8. Безпека даних в IP-мережах

Загрози процедурам адресації. Одними з найважливіших показників сучасних телекомунікаційних мереж звісно є надійність, відмовостійкість і вартість. Однак, останнім часом все більш актуальною є безпека телекомунікаційної мережі, яка впливає на безпеку конфіденційних даних, які можуть оброблюватись та зберігатись в апаратно-програмному середовищі ТКМ. Сьогодні безпека інформації в мережах є проблемою, яка постійно буде вирішуватись але ніколи не буде вирішеною на сто відсотків [3; 8; 10; 15 – 17; 21; 25; 26; 39; 41 – 45]. В зв'язку з цим необхідно мати уявлення про існуючі механізми забезпечення безпеки інформації та порядок їх використання на практиці. Розглянемо особливості процесів пов'язаних з адресацією і маршрутизацією в сучасних телекомунікаційних мережах, які можуть служити базою для здійснення порушень безпеки інформації в мережах.

Розповсюдженим стеком протоколів, звісно, є стек TCP/IP, тому проаналізуємо його захищеність та надійність. Розглянемо звичайний заголовок IP-дейтаграми без параметрів (рис. 7.14).

Версія	Довжина заголовка	Тип обслуговування	Загальна довжина
Ідентифікатор			Зсув фрагменту
TTL (час життя)		Протокол	Контрольна сума заголовка
IP-адреса відправника			
IP-адреса отримувача			

Рис. 7.14. Заголовок IP-дейтаграми без параметрів

Із усіх полів заголовку IP значущим є поле Протокол. Воно вказує на тип протоколу, який використовувався для інкапсуляції. Наприклад, значення 17, у шістнадцятирічному виді 11, означає, що на транспортному рівні використовується протокол UDP, значення 6 – вбудованим пакетом є TCP-пакет, значення 1 – відповідає ICMP-пакету.

Звісно, що IP-адреса (довжина 4 байта) є логічною, фізичною адресою хоста є MAC-адреса (довжиною 6 байт), яка зберігається в мережевій карті. Тому при передачі даних в локальній мережі використовуються фізичні адреси, які встановлюють за IP-адресами і навпаки протоколи ARP, RARP.

Адресація має суттєве значення при забезпеченні безпеки в комп'ютерних і телекомунікаційних мережах. Зміна адрес, використання невірних адрес є однією з загроз безпеки сучасних мереж. Сучасні операційні системи для обміну даними в мережах крім логічних і фізичних адрес використовують адреси програмних і апаратних портів (номера 2 байта). Номера портів записуються у відповідні поля заголовків пакетів протоколів IP і TCP. Існує 65536 варіантів портів. Частина з яких записана за конкретними службами, наприклад:

ftp – 21/tcp, telnet – 23/tcp, smtp – 25/tcp, domain – 53/udp, domain – 53/tcp.

Тому для зловмисника привабливим варіантом здійснення несанкціонованого доступу буде використання деякого порта, який не прописаний за певною службою по замовчуванню.

Наприклад, в заголовку UDP-пакету міститься 2-байтове поле під назвою поле отримувача, в якому визначається порт 53, тобто дейтаграма призначена службі domain. Для більшої безпеки сьогодні особливу увагу привертають до портів з номерами більш за 1024, які використовують як тимчасові. Найвищим рівнем в ієрархії адрес є використання доменних імен (dns-імен). DNS – Domain Name System – система доменних імен. Призначенням цієї служби є полегшення роботи користувачів мереж, шляхом створення dns-таблиць, або розподілених баз даних, в яких містяться адреси серверів та хостів і їх відповідні доменні імена.

Загрози процедурам маршрутизації.

Процедури маршрутизації можна розділити на дві категорії: протоколи типу IGP (Interior Gateway Protocol – протокол внутрішнього шлюзу) і протоколи типу EGP (External Gateway Protocol – протокол зовнішнього шлюзу). IGP призначений для маршрутизації трафіку між комп'ютерами автономної системи (ієрархічна сукупність маршрутизаторів). IGP протоколами є протоколи RIP (Routing Information Protocol) і OSPF (Open Shortest Path First). RIP і OSPF підтримується практично усіма маршрутизаторами і відрізняються методами отримання поновленої маршрутної інформації і критеріями пошуку найкращих маршрутів.

Протоколи EGP необхідні для передачі пакетів між автономними системами. Ці протоколи дозволяють зв'язати окремі автономні системи в єдину мережу. Відомим EGP-протоколом є BGP (Border Gateway Protocol – протокол межового шлюзу). Сьогодні BGP-сервери на магістральних лініях Internet підтримують таблиці маршрутизації, в яких зберігаються адреси усіх зовнішніх маршрутів Internet.

Основною загрозою для сучасних телекомунікаційних мереж є створення зловмисником хибних маршрутів, несанкціонована зміна маршрутної

інформації, що приводить до зміни напрямку потоків даних і їх можливого знищенню. Існуючі механізми дозволяють закривати частину даних, яка стосується напрямків слідування даних скрізь мережі, створювати так звані віртуальні мережі, що дозволяє забезпечувати захист інформації від певних загроз безпеки.

Для аналізу трафіку певної машини поширеним програмним пакетом є tcpdump і lippcup, які доступні за адресами <ftp://ftp.ee.lbl.gov/tcpdump.tar.Z> і <ftp://ftp.ee.lbl.gov/lippcup.tar.Z> відповідно. Розглянуті загрози сьогодні можливо відносно нейтралізувати шляхом використання програмно-апаратних мережевих сканерів, антивірусних програм та Firewall-ів.

Контрольні запитання

1. Скільки рівнів і які входять до стеку TCP/IP?
2. Які функції виконує рівень міжмережної взаємодії стека TCP?
3. З якою метою використовують маску під мережі?
4. Що таке маршрут?
5. З якою метою у протоколі RIP обмежено кількість пересилань?
6. Поясніть поняття: «хост-мережа», «тупикова мережа», «транзитна мережа»?
7. Які функції виконує протокол SAP?
8. Призначення поля «керування транспортом» пакета IPX?
9. Поясніть принцип одно крокової маршрутизації IPX-маршрутизаторів?
10. На яких рівнях моделі OSI працює протокол NetBIOS?
11. Яку функцію виконує сервіс повідомлень SMB?
12. На яких рівнях моделі OSI працює протокол Apple Talk?
13. Що таке віддалений виклик процедур у архітектурі NetWare?
14. У чому полягають особливості протоколів архітектури SNA?
15. Що є основним комутаційним елементом мережної архітектури DNA?
16. З якою метою у заголовку IP дейтаграми використовують поле TTL (час життя)?
17. Які загрози можуть виникати процедурам маршрутизації?

РОЗДІЛ 8. СТЕК ПРОТОКОЛІВ TCP/IP

8.1. Базова модель TCP/IP

Стек протоколів – це група взаємозалежних протоколів, необхідних для виконання функції зв'язку.

Один з найкращих способів візуалізації взаємодії протоколів у стеці – це аналіз їх сукупної взаємодії. Стек протоколів показує, як реалізуються окремі протоколи з певного набору. Протоколи розглядаються з точки зору рівнів, кожен сервіс вищого рівня залежить від функціональності, визначеної протоколами нижчих рівнів. Нижні рівні стека відповідають за передавання даних через мережу та надання сервісів верхнім рівням, які відповідають за зміст повідомлень, що передаються.

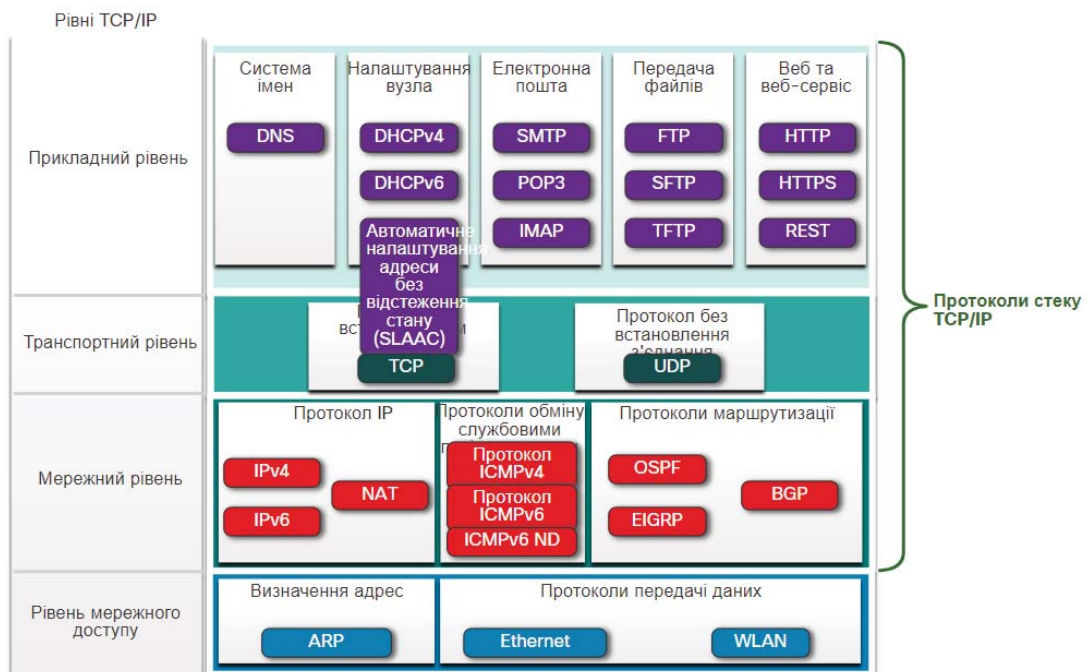


Рис. 8.1. Стек протоколів TCP/IP

Стек інтернет-протоколів або стек TCP/IP – це найпоширеніший і найвживаніший стек протоколів, що застосовується сьогодні. Стек протоколів TCP/IP – це відкритий стандартний набір протоколів, що підтримується Інженерною робочою групою (IETF, Internet Engineering Task Force) [27].

Сьогодні набір протоколів TCP/IP містить багато протоколів і продовжує розвиватися для підтримки нових інформаційних послуг. Деякі з найбільш вживаних протоколів зображені на рисунку.

TCP/IP – це стек протоколів, що використовується в сучасних мережах та мережі Інтернет. TCP/IP має два важливих аспекти для постачальників та виробників:

- *Відкритий стандартний набір протоколів* – це означає, що він знаходиться у вільному доступі для громадськості і може бути використаний будь-яким постачальником на власному обладнанні або у власному програмному забезпеченні.
- *Набір протоколів на основі стандартів* – це означає, що він був схвалений мережевий індустрією і схвалений організацією зі стандартизації. Це гарантує, що продукти від різних виробників будуть успішно взаємодіяти між собою.

Таблиця 8.1.

Опис рівнів моделі TCP/IP

<i>Рівні моделі TCP/IP</i>	<i>Опис</i>
<i>4 – Прикладний рівень</i>	Відображення даних для користувача, а також забезпечення шифрування та керування сеансами зв'язку.
<i>3 – Транспортний рівень</i>	Підтримка зв'язку між різними пристроями в різних мережах.
<i>2 – Міжмережний рівень</i>	Визначення найкращого маршруту передавання даних через мережу.
<i>1 – Рівень мережного доступу</i>	Керування фізичними пристроями та середовищем передавання даних, з яких складається мережа.

Еталонна модель OSI надає великий перелік функцій і сервісів, які можуть бути присутніми на кожному рівні. Модель цього типу забезпечує узгодженість усіх типів мережних протоколів та служб, описуючи, що необхідно зробити на певному рівні, але не визначаючи, як це потрібно виконати.

Протокольна модель TCP/IP, як модель для міжмережного зв'язку була створена на початку 1970-х років. Іноді її називають моделлю мережі Інтернет. Модель цього типу тісно пов'язана зі структурою відповідного стеку протоколів. TCP/IP – протокольна модель, оскільки вона описує

функції, які виконуються на кожному рівні стеку TCP/IP. TCP/IP також використовується як еталонна модель. У таблиці наведена детальна інформація про рівні моделі OSI.

Визначення стандарту та протоколів TCP/IP обговорені на загальнодоступному форумі та описані в загальнодоступному набір документів RFC, виданих IETF. RFC створюються мережними інженерами і надсилаються іншим членам IETF для обговорення.

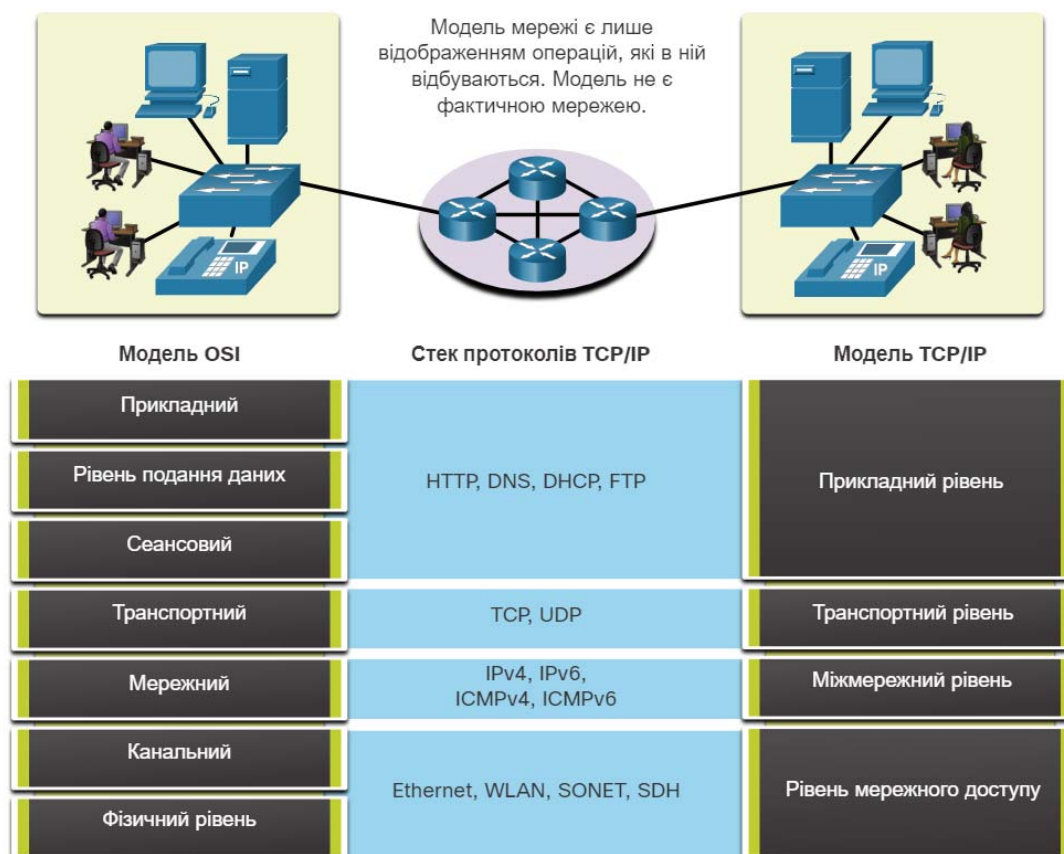


Рис. 8.2. Співставлення рівнів моделей

8.2. Протоколи прикладного рівня

Протоколи прикладного рівня TCP / IP визначають формати і управляють даними, необхідними для багатьох поширених функцій обміну даними через Інтернет.

Доменна система імен

- *DNS, Domain Name System* – доменна система імен. Визначає IP-адреси, що відповідають доменним іменам (наприклад, IP-адреси для сайту cisco.com).

Протоколи налаштування вузла

- *DHCPv4, Dynamic Host Configuration Protocol for IPv4* – протокол динамічного налаштування вузла для IPv4. Сервер DHCPv4 динамічно надає інформацію про адресацію IPv4 клієнтам DHCPv4 при запуску і дозволяє повторно використовувати адреси, коли вони більше не потрібні.
- *DHCPv6, Dynamic Host Configuration Protocol for IPv6* – протокол динамічного налаштування вузла для IPv6. DHCPv6 подібний на DHCPv4. Сервер DHCPv6 динамічно надає інформацію про адресацію IPv6 клієнтам DHCPv6 при запуску.
- *SLAAC, Stateless Address Autoconfiguration* – автоматичне налаштування адреси без відстеження стану. Метод, який дозволяє пристрою отримувати адресну інформацію IPv6 без використання сервера DHCPv6.

Протоколи електронної пошти

- *SMTP, Simple Mail Transfer Protocol* – простий протокол електронної пошти. Дозволяє клієнтам надсилати email-повідомлення на поштовий сервер, а серверам - на інші сервери.
- *POP3, Post Office Protocol version 3* – поштовий протокол версії 3. Дозволяє клієнтам отримувати електронну пошту з поштового сервера та завантажувати електронну пошту до локальної поштової програми клієнта.
- *IMAP, Internet Message Access Protocol* – протокол доступу до інтернет-повідомлень. Дозволяє клієнтам отримувати доступ до електронної пошти, що зберігається на поштовому сервері, а також зберігати електронну пошту на сервері.

Протоколи передавання файлів

- *FTP, File Transfer Protocol* – протокол передавання файлів. Встановлює правила, які дозволяють користувачу одного хоста мати доступ до файлів та передавати файли з іншого хоста через мережу FTP - надійний, орієнтований на з'єднання протокол гарантованої доставки файлів
- *SFTP, Secure Shell FTP* – безпечний протокол передавання файлів. Протокол SFTP є розширенням протоколу SSH та може застосовується для організації безпечного сеансу передавання файлів. SSH – метод безпечного віддаленого входу, який зазвичай використовується для доступу до командного рядка пристрою.
- *TFTP, Trivial FTP* – простий протокол передавання файлів. TFTP – це простий протокол передавання файлів без встановлення з'єднання, який докладає зусиль для доставки, але її не гарантує. У порівнянні з FTP має менші накладні витрати.

Протоколи Веб та веб-сервісів

- *HTTP, Hypertext Transfer Protocol* – протокол передавання гіпертекстових повідомлень. Набір правил для обміну текстом, графічними зображеннями, аудіо, відео та іншими мультимедійними файлами у всесвітній мережі.
- *HTTPS, HTTP Secure* – Захищений HTTP. Безпечний варіант HTTP, що шифрує дані, якими обмінюються вузли через всесвітню мережу (WWW, World Wide Web).
- *REST, Representational State Transfer* – передавання репрезентативного стану. Веб-сервіс, який використовує інтерфейси прикладного програмування (APIs, Application Programming Interfaces) та HTTP-запити для створення веб-застосунків.

8.2.1 DNS (Служба доменних імен)

На прикладному рівні спеціально визначені протоколи для полегшення процесу отримання адрес мережними пристроями. Ці сервіси важливі, оскільки запам'ятовування IP-адрес, що відповідають URL, або налаштування мережних параметрів на усіх пристроях у мережі середніх і великих розмірів вимагало би багато часу і зусиль.

Для надсилання і отримання даних по мережі пристрої позначаються спеціальними числовими IP-адресами. Доменні імена були створені для перетворення числової адреси на просту, впізнавану назву.

При роботі в інтернеті, набагато легше запам'ятати повнокваліфіковані доменні імена (fully-qualified domain names, FQDNs), такі як <http://www.cisco.com>, аніж фактичну числову адресу сервера 198.133.219.25. Якщо компанія Cisco вирішить змінити числову адресу www.cisco.com, це відбудеться непомітно для користувачів, оскільки доменне ім'я не зазнає змін. Нова адреса буде просто прив'язана до існуючого доменного імені без порушення зв'язку із сервером.

Протокол DNS визначає автоматизований сервіс, який зіставляє імена інтернет-ресурсів із відповідними числовими мережними адресами. Для обміну даними протокол DNS використовує єдиний формат, який називається повідомленням. Він включає формат запитів, відповідей і дані. Такий формат повідомлення використовується для усіх типів клієнтських запитів, відповідей від серверів, повідомлень про помилки та при перенаправленні ресурсних записів між серверами.

Формат DNS-повідомлень

На DNS-серверах зберігаються різні типи ресурсних записів, які використовуються для перетворення імен. Ці записи містять ім'я, адресу та тип запису. До таких типів записів належать:

- **A** – Адреса кінцевого пристрою IPv4
- **NS** – Авторитетний сервер імен
- **AAAA** – Адреса IPv6 кінцевого пристрою (вимовляється як "куад Ей")
- **MX** – Запис для поштового сервера домену

При надходженні звернення від клієнта, процес DNS-сервера спочатку переглядає власні записи у спробі перетворити запитане ім'я. Якщо розпізнати ім'я, використовуючи збережені записи, не вдається, сервер звертається до інших серверів задля перетворення. Після того, як відповідність знайдено і числова адреса повертається серверу, який надсилав запит, він тимчасово зберігатиме цю адресу на випадок повторного надходження запиту з тим самим іменем.

Клієнтський сервіс DNS на ПК з ОС Windows також зберігає у пам'яті попередньо перетворені імена. Команда `ipconfig /displaydns` зображає всі кешовані DNS-записи.

DNS використовує однаковий формат повідомлень, який складається із запитання, відповіді, авторитетного джерела і додаткової інформації, для усіх типів запитів клієнтів і відгуків серверів. а також передавання ресурсних записів між серверами (табл. 8.2).

Таблиця 8.2.

Розділи DNS-повідомлень

Розділи DNS-повідомлень	Опис
Запитання	Запитання до сервера імен
Відповідь	Ресурсні записи, які відповідають на запитання
Авторитетне джерело	Ресурсні записи, які вказують на джерело
Додатковий	Ресурсні записи, що містять додаткову інформацію

Ієрархія DNS

Протокол DNS використовує ієрархічну систему для створення бази даних, що забезпечує перетворення імен. При формуванні ієрархії DNS використовує доменні імена (рис. 8.3).

Структура іменування розбита на невеликі, контрольовані зони. Кожен DNS-сервер підтримує певний файл бази даних і відповідає лише за зіставлення імен з IP для цієї невеликої частини всієї структури DNS. Коли DNS-сервер отримує запит на переклад імені, яке не належить до його DNS-зони, він перенаправляє запит щодо перетворення на інший DNS-сервер у межах відповідної зони. DNS масштабується, оскільки розпізнавання імені вузла поширюється на декілька серверів.

Різні домени верхнього рівня позначають тип організації або країну походження. Приклади доменів верхнього рівня:

- **.com** – бізнес або промисловість
- **.org** – некомерційна організація
- **.au** – Австралія
- **.co** – Колумбія

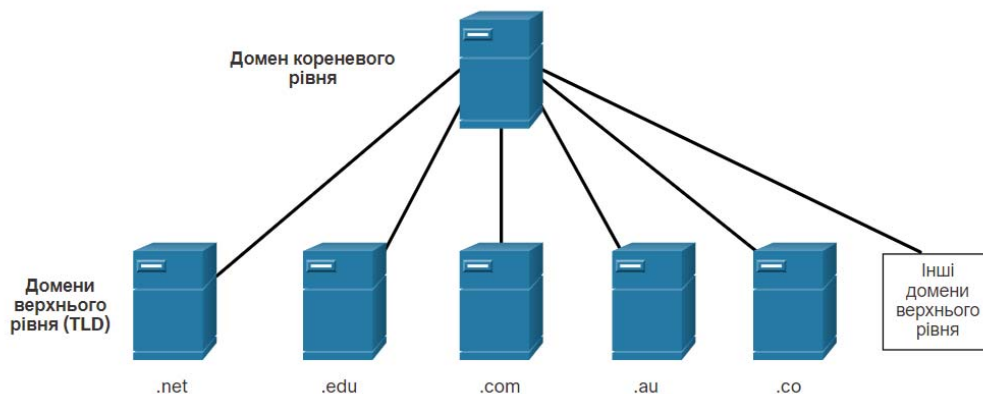


Рис. 8.3. Ієрархія DNS

8.2.2 Протокол динамічного налаштування вузла DHCP

Протокол динамічного налаштування вузла (Dynamic Host Configuration Protocol, DHCP) для IPv4 автоматизує призначення IPv4-адрес, масок підмереж, шлюзів та інших мережних параметрів IPv4. Цей процес називають динамічною адресацією, альтернативною до якої є статичне призначення мережних параметрів. При використанні статичної адресації адміністратор мережі вручну вводить інформацію про IP-адреси на вузлах.

В умовах динамічної адресації при під'єднанні до мережі, вузол звертається до DHCP-сервера і запитує адресу. DHCP-сервер обирає адресу

із налаштованого діапазону адрес, який називають пулом, і призначає її (передає у тимчасове користування) вузлу.

У великих мережах або в умовах постійної зміни кількості користувачів, DHCP вважається ефективним рішенням для призначення адрес. Нові користувачі або пристрої можуть періодично додаватися і потребувати мережного з'єднання. Замість того, щоб використовувати статичну адресацію для кожного підключення, ефективніше призначати IPv4-адреси автоматично за допомогою DHCP.

DHCP може надавати IP-адреси на певний періоду часу - період оренди, який можна налаштовувати. Період оренди є важливим параметром DHCP. Коли він закінчується або DHCP-сервер отримує від клієнта повідомлення DHCPRELEASE, надана адреса повертається до пулу DHCP для повторного використання. Завдяки DHCP користувачі можуть вільно переміщатися з місця на місце і легко відновлювати мережне з'єднання.

Як показано на рисунку, роль серверів DHCP можуть виконувати різні типи пристроїв. У більшості мереж середнього і великого розміру DHCP-сервер – це, зазвичай, локальний виділений сервер на базі ПК. Для домашніх мереж DHCP-сервер традиційно розгортається на локальному маршрутизаторі, який під'єднує домашню мережу до інтернет-провайдера.

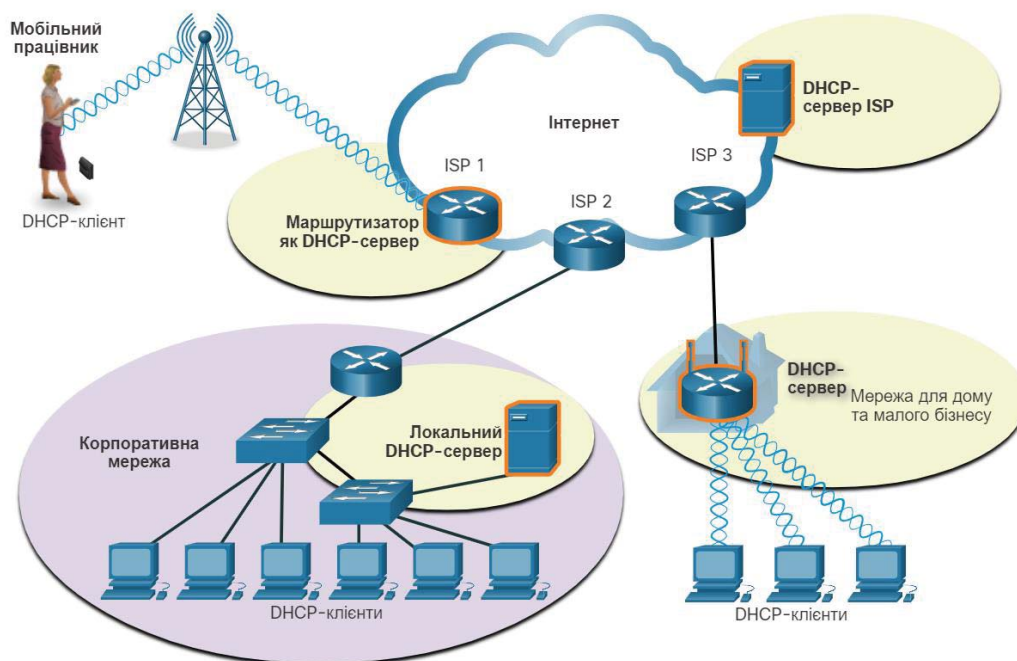


Рис. 8.4. Сервери DHCP

Принципи роботи протоколу DHCP

Як показано на рисунку, при запуску або під'єднанні до мережі пристрою IPv4 з підтримкою DHCP, його клієнтська частина надсилає широкомовне повідомлення DHCPDISCOVER для виявлення будь-яких DHCP-серверів, наявних у мережі. DHCP-сервер відповідає повідомленням DHCPOFFER, у якому пропонує клієнту орендувати деякі параметри. Повідомлення з пропозицією містить IPv4-адресу та маску підмережі, IPv4-адресу DNS-сервера та IPv4-адресу шлюзу за замовчуванням, готові для призначення. Пропозиція також містить термін оренди.

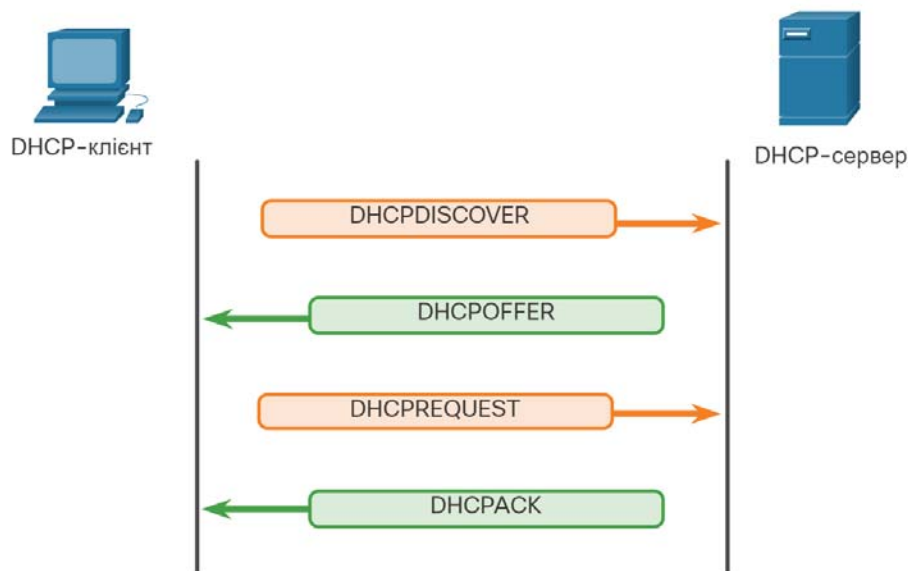


Рис. 8.5. Принципи роботи протоколу DHCP

Клієнт може отримати декілька повідомлень DHCPOFFER за наявності в локальній мережі більше одного DHCP-сервера. У цьому випадку клієнт має обрати одну з пропозицій, і надіслати DHCP-запит (DHCPREQUEST) із зазначенням конкретного сервера та пропозиції оренди, яку він приймає. Клієнт також може запросити адресу, яку раніше йому надавав сервер.

Якщо адреса IPv4, яку запитує клієнт або пропонує сервер, все ще доступна, сервер повертає повідомлення з підтвердженням DHCP (DHCPACK), яке засвідчує надання в оренду вказаних параметрів. Якщо пропозиція більше недійсна, обраний сервер відповідає повідомленням про негативне підтвердження DHCP (DHCPNAK). У разі повернення повідомлення DHCPNAK, процес вибору повинен розпочатися заново з надсилання нового повідомлення DHCPDISCOVER. Після того, як клієнт отримав у тимчасове користування адресу, він має подовжити її оренду до

закінчення терміну дії за допомогою ще одного повідомлення DHCPREQUEST.

DHCP-сервер забезпечує унікальність усіх IP-адрес (однакові IP-адреси не можуть бути призначені одночасно двом різним мережним пристроям). Більшість інтернет-провайдерів використовують DHCP для надання адрес своїм клієнтам.

DHCPv6 також має набір повідомлень, аналогічний до DHCPv4, зокрема таких як: SOLICIT, ADVERTISE, INFORMATION REQUEST, та REPLY.

8.2.3 Протоколи HTTP та HTTPS

HTTP – це протокол типу "запит-відповідь". Коли клієнт, зазвичай веб-браузер, надсилає запит до веб-сервера, HTTP зазначає типи повідомлень, які використовуються у цьому з'єднанні. Традиційно це три типи повідомлень: GET (див. рисунок), POST і PUT:

- *GET* – Запит даних клієнтом. Клієнт (веб-браузер) надсилає повідомлення GET веб-серверу як запит HTML-сторінок.
- *POST* – Розміщення файлів даних на веб-сервері, наприклад даних форми.
- *PUT* – Розміщення на веб-сервері ресурсів або контенту, наприклад, зображень.

Хоча HTTP є надзвичайно гнучким протоколом, він не є безпечним. Повідомлення із запитом передають інформацію на сервер у відкритому вигляді, а отже їх можна перехопити і прочитати. Відповіді сервера, зазвичай HTML-сторінки, також не шифруються.

Для підтримки безпечного з'єднання через Інтернет використовується протокол HTTP Secure (HTTPS). HTTPS використовує автентифікацію та шифрування для захисту даних під час їх переміщення між клієнтом і сервером. HTTPS використовує той самий процес "запит-відповідь" між клієнтом і сервером, що і HTTP, але перш ніж ширитися мережею, потік даних шифрується за допомогою протоколу Secure Socket Layer (SSL).

8.2.4 Протокол передавання файлів (FTP)

Як ви дізналися у попередніх темах, у моделі клієнт-сервер клієнт має змогу розміщувати дані на сервері, та завантажувати дані з сервера, якщо обидва пристрої використовують протокол передавання файлів (FTP, File

Transfer Protocol). Як і протоколи HTTP, електронної пошти та адресації, FTP є одним із традиційних протоколів прикладного рівня.

FTP розроблений для обміну даними між клієнтом і сервером. FTP-клієнт – це застосунок, який працює на комп'ютері для завантаження даних з FTP-сервера і передавання даних на нього.

Клієнт зв'язується із сервером по мережі. Перше повідомлення від клієнта – це керуюче з'єднання: клієнт спершу утворює зв'язок із сервером для контролю трафіку. Друге повідомлення від клієнта - це передавання даних: клієнт відкриває друге з'єднання для трафіку даних. Клієнт запитує дані з сервера за допомогою команди Get Data.

Клієнт встановлює перше з'єднання із сервером для керування трафіком, використовуючи TCP-порт 21. Трафік складається з клієнтських команд і відповідей сервера.

Клієнт встановлює друге з'єднання з сервером для фактичного передавання даних, використовуючи TCP-порт 20. Це з'єднання створюється щоразу при появі даних для надсилання.

Обмін даними може відбуватися у будь-якому напрямку. Клієнт може завантажувати (pull) дані з сервера або передавати (push) дані на сервер.

8.2.5. Протоколи обробки електронної пошти SMTP, POP3, IMAP4

Хостинг електронної пошти – це одна з основних послуг, яку надають провайдери інтернет-послуг. Як показано на рисунку, використання на комп'ютері або іншому кінцевому пристрої засобів електронної пошти потребує деяких програм і сервісів. Електронна пошта (email) – це спосіб передавання, зберігання і отримання електронних повідомлень у мережі. Повідомлення електронної пошти зберігаються у базах даних на поштових серверах.

Клієнти електронної пошти для надсилання та отримання повідомлень з'єднуються з поштовими серверами. Мережні сервери взаємодіють між собою для пересилання повідомлень з одного домену на інший. Під час обміну електронними повідомленнями email-клієнти безпосередньо не спілкуються один з одним. Замість цього для передавання повідомлень обидва клієнти покладаються на поштовий сервер.

Роботу електронної пошти підтримують три окремі протоколи: Simple Mail Transfer Protocol (SMTP), Post Office Protocol (POP), та IMAP. Процес прикладного рівня, який надсилає пошту, використовує SMTP. Отримання

клієнтом електронних повідомлень, відбувається завдяки одному з двох протоколів прикладного рівня: POP або IMAP.

SMTP

SMTP-повідомлення складається із заголовку і тіла. Якщо тіло повідомлення може містити текст довільного обсягу, заголовок повідомлення повинен включати email-адреси одержувача і відправника визначеного формату.

Коли клієнт надсилає повідомлення електронної пошти, SMTP-процес клієнта з'єднується з SMTP-процесом сервера через відомий порт 25. Після встановлення з'єднання, клієнт намагається надіслати email-повідомлення на сервер. Коли сервер отримує повідомлення, він або розміщує повідомлення у локальній поштової скриньці, якщо одержувач є користувачем цього сервера, або пересилає повідомлення на інший поштовий сервер для доставки.

При надсиланні електронного повідомлення, email-сервер призначення може бути зайнятий або не на зв'язку. Тому, SMTP розміщує повідомлення у чергу аби надіслати пізніше. Періодично сервер перевіряє чергу повідомлень і намагається повторно їх передати. Якщо повідомлення все ще не було надіслане, по закінченню визначеного терміну, воно повертається відправникові як таке, що неможливо доставити.

POP

POP використовується застосунком для отримання email-повідомлень з поштового сервера. За допомогою POP пошта завантажується на бік клієнта, після чого видаляється із сервера. У такий спосіб POP працює за замовчуванням.

Сервер запускає сервіс POP, пасивно прослуховуючи TCP-порт 110 щодо надходження запитів від клієнтів. Як показано на рисунку, коли клієнт хоче скористатися цією послугою, він надсилає запит на встановлення TCP-з'єднання із сервером. Після налаштування з'єднання сервер POP надсилає привітання. Далі клієнт і POP-сервер обмінюються командами і відповідями, до закриття або переривання з'єднання.

При використанні POP повідомлення електронної пошти завантажуються до клієнтської програми і видаляються із сервера, а отже, використання цього протоколу не передбачає централізованого зберігання email-повідомлень. Оскільки POP не зберігає повідомлення, його

використання небажане для невеликих підприємств, які потребують централізованого рішення для резервного копіювання.

Найчастіше використовується версія POP3.

IMAP

IMAP – це ще один протокол, який описує спосіб отримання повідомлень електронної пошти. На відміну від POP, при зверненні користувача до сервера з підтримкою IMAP, копії повідомлень завантажуються до клієнтського застосунку, як зображено на рисунку. Оригінальні повідомлення зберігаються на сервері, поки не будуть видалені вручну. Користувачі переглядають копії повідомлень у клієнтській програмі електронної пошти і можуть створювати на сервері ієрархію файлів для впорядкування та зберігання електронних листів. Ця файлова структура також дублюється на поштовому клієнті. Коли користувач вирішує видалити повідомлення, сервер синхронізує цю дію і видаляє повідомлення у себе.

8.2.6. Telnet, SSH та SNMP

Протокол Telnet був реалізований у середовищі Unix і, поряд з електронною поштою та FTP доступами до архівів файлів, був популярним сервісом Інтернету. Однак, оскільки для автентифікації користувачів у технології Telnet застосовуються паролі, що передаються через мережу у вигляді звичайного тексту (що означає, що паролі можуть бути легко перехоплені та використані), Telnet зараз працює переважно в межах однієї локальної мережі, де можливостей для перехоплення пароля набагато менше. Для віддаленого керування вузлами через Інтернет замість Telnet зазвичай застосовується протокол SSH (Secure SHell). який, як і Telnet, спочатку був розроблений для ОС Unix1. SSH, як і Telnet, передає символи, що набираються на терміналі користувача, на віддалений вузол без інтерпретації їх змісту. Однак SSH забезпечує захист віддалених з'єднань, надаючи надійне шифрування даних автентифікації пристрою (ім'я користувача та пароль), а також даних, що передаються між пристроями. SSH використовує TCP-порт 22. Telnet використовує TCP-порт 23.

Сьогодні основною сферою застосування Telnet є керування не комп'ютерами, а комунікаційними пристроями: маршрутизаторами, комутаторами та хабами. Таким чином, він уже скоріше є не

користувальницьким протоколом, а протоколом адміністрування, тобто альтернативою SNMP.

Проте відмінність між протоколами Telnet та SNMP є принциповою. Простий протокол керування мережами (SNMP, Simple Network Management Protocol) використовується для моніторингу мережі. Telnet передбачає обов'язкову участь людини в процесі адміністрування, оскільки, по суті, лише транслює команди, які вводить адміністратор при конфігуруванні або моніторингу маршрутизатора (іншого комунікаційного пристрою). Протокол SNMP, навпаки, розрахований на автоматичні процедури моніторингу та управління, хоч і не виключає можливості участі адміністратора у цьому процесі. Для усунення небезпеки, що породжується передачею паролів у відкритому вигляді через мережу, комунікаційні пристрої посилюють ступінь свого захисту. Зазвичай використовується багаторівнева схема доступу, коли відкритий пароль дає змогу лише читати базові характеристики конфігурації пристрою, а доступ до засобів зміни конфігурації вимагає іншого пароля, який вже не передається у відкритому вигляді.

Протокол SNMP використовується як стандартний протокол взаємодії менеджера та агента. Протокол SNMP відноситься до прикладного рівня стека TCP/IP.

Для транспортування своїх повідомлень він використовує дейтаграмний транспортний протокол UDP, який, як відомо, не забезпечує надійної доставки. Протокол TCP, який організовує надійну передачу повідомлень на основі з'єднань, дуже завантажує керовані пристрої, які на момент розробки протоколу SNMP були не дуже потужні, тому від протоколу TCP було вирішено відмовитися. SNMP – це протокол типу "запит-відповідь", тобто на кожен запит, що надійшов від менеджера, агент повинен передати відповідь. Особливістю протоколу є його надзвичайна простота — він включає всього кілька команд:

- Команда `GetRequest` використовується менеджером для запиту агента про значення будь-якої змінної за її стандартним ім'ям.
- Команда `GetNextRequest` застосовується менеджером для отримання значення наступного об'єкта (без вказівки його імені) при послідовному перегляді таблиці об'єктів.
- За допомогою команди `Response` SNMP-агент передає менеджеру відповідь на команду `GetRequest` або `GetNextRequest`.
- Команда `SetRequest` дозволяє менеджеру змінювати значення будь-якої змінної або списку змінних. За допомогою команди `SetRequest` і

відбувається власне керування пристроєм. Агент повинен «розуміти» зміст значень змінної, яка використовується для керування пристроєм, і на підставі цих значень ви виконувати реальний керуючий вплив – відключити порт, приписати порт певної лінії VLAN тощо. Команда `SetRequest` придатна також для завдання умови, при виконанні якого SNMP-агент повинен надіслати менеджеру відповідне повідомлення. Таким чином, може бути визначена реакція на такі події, як ініціалізація агента, рестарт агента, обрив зв'язку, відновлення зв'язку, неправильна автентифікація та втрата найближчого маршрутизатора. Якщо відбувається будь-яка з цих подій, агент ініціалізує переривання.

- Команда `Trap` використовується агентом для повідомлення менеджеру про виникнення особливої ситуації.
- Команда `GetBulk` дозволяє менеджеру отримати кілька змінних за один запит.

SNMP-повідомлення, на відміну від повідомлень багатьох інших комунікаційних протоколів, не мають заголовків з фіксованими полями. Будь-яке SNMP-повідомлення складається з трьох основних частин: версії протоколу, загального рядка та області даних.

Загальний рядок (`community string`) використовується для групування пристроїв, керованих певним менеджером. Загальний рядок є свого роду паролем, оскільки для того, щоб пристрої могли взаємодіяти за протоколом SNMP, вони повинні мати те саме значення цього ідентифікатора (за умовчанням часто використовується рядок «`public`»). Однак цей механізм служить скоріше для «розпізнавання» партнерів, ніж безпеки.

В області даних містяться описані команди протоколу, а також імена об'єктів та їх значення. Область даних складається з одного або більше блоків, кожен з яких може належати до одного з перерахованих типів команд протоколу SNMP. Для кожного типу команди визначено свій формат [2].

8.3. Протоколи транспортного рівня

Протокол IP відповідає тільки за структуру, адресацію та маршрутизацію пакетів. IP не визначає яким чином здійснюється доставка або транспортування пакетів.

Протоколи транспортного рівня визначають спосіб передавання повідомлень між вузлами, і відповідають за керування вимогами надійності

діалогу. Основним завданням транспортного рівня стека TCP/IP є взаємодія між прикладними програмами.

Транспортний рівень виконує дві функції:

- Управляє потоком;
- Гарантує надійність передачі.

Для цього в TCP/IP використаний механізм підтвердження правильного прийому з дублюванням передачі загублених пакетів або пакетів, що надійшли з помилками. Транспортний рівень приймає дані від декількох прикладних програм і надсилає їх нижньому рівню. При цьому він долучає додаткову інформацію до кожного пакета, у тому числі контрольну суму [10]. В основі транспортного рівня стека TCP/IP лежить TCP (Transmission Control Protocol) – протокол керування передачею, що працює з установкою логічного з'єднання між віддаленими прикладними процесами, а також використовує принцип автоматичної повторної передачі пакетів, які містять помилки [4].

Різні застосунки висувають різні вимоги щодо надійності послуг транспортного рівня. З огляду на це, TCP/IP надає два протоколи транспортного рівня:

- *TCP, Transmission Control Protocol (протокол керування передаванням)* – протокол зі встановленням з'єднання і квітунням. Він відповідає за розбиття повідомлень на сегменти, їх збирання у вузлі призначення, повторне відсилення всього, що виявилось неотриманим, і збирання повідомлень із сегментів. Протокол TCP забезпечує гарантовану доставку даних за рахунок утворення логічних (віртуальних) з'єднань між віддаленими прикладними процесами;

- *UDP (User Datagram Protocol, протокол дейтаграм користувача)*, не орієнтований на встановлення з'єднання. Хоча протокол UDP і відповідає за передачу повідомлень, на цьому рівні квітуння не застосовується, оскільки відсутнє програмне забезпечення для перевірки доставки сегментів.

8.3.1 Протокол TCP

IP опікується виключно структурою, адресацією та маршрутизацією пакетів від початкового відправника до кінцевого пункту призначення. IP не несе відповідальності за гарантування доставки або визначення того, чи потрібно налагодити зв'язок між відправником і одержувачем.

TCP вважається надійним повнофункціональним протоколом транспортного рівня, який гарантує доправлення всіх даних до пункту призначення. TCP включає поля, які забезпечують доставку даних застосунків. Ці поля вимагають додаткової обробки з боку вузлів відправника і отримувача. TCP виконує розбиття даних на сегменти.

Транспортування TCP подібне до надсилання посилок з відстеженням від джерела до пункту призначення. Якщо розбити замовлення на декілька пакунків, клієнт зможе в онлайн-режимі відстежувати порядок їх доставки.

TCP забезпечує надійність і керування потоком за допомогою таких основних операцій:

- Нумерація та відстеження сегментів даних, переданих конкретному вузлу від визначеного застосунку.
- Підтвердження отриманих даних.
- Повторне надсилання будь-яких непідтверджених даних через певний проміжок часу.
- Відновлення послідовності даних, які могли надійти у неправильному порядку.
- Надсилання даних з ефективною швидкістю, прийнятною для одержувача.

Аби підтримувати стан діалогу та відстежувати інформацію, TCP потрібно спочатку налагодити зв'язок між відправником і одержувачем. Саме тому TCP відомий як протокол, орієнтований на з'єднання.

Натисніть кнопку «Відтворити» на рисунку, щоб побачити, як TCP-сегменти та підтвердження про доставку передаються між відправником та одержувачем.

Крім підтримки основних функцій сегментації і відтворення порядку надсилання даних, TCP також надає такі послуги:

- *Встановлює сеанс* – TCP – це орієнтований на з'єднання протокол, який перш ніж розпочати пересиланням будь-якого трафіку узгоджує умови і встановлює постійне з'єднання (або сеанс) між пристроями джерела і призначення. Через створення сеансу пристрої узгоджують обсяг трафіку, який може бути надісланий у даний момент часу, а процес передавання даних між ними можна ретельно контролювати.
- *Забезпечує надійну доставку* – В процесі передавання мережею з багатьох причин, може трапитися пошкодження або повна втрата сегментів. TCP гарантує, що кожен сегмент, який надсилається джерелом, надходить до пункту призначення.

- *Забезпечує впорядковану доставку* – Оскільки у мережі може існувати декілька шляхів для надсилання даних з різними швидкостями, дані можуть надходити в неправильному порядку. Через нумерування та відстеження послідовності сегментів, TCP гарантує, що при отриманні належний порядок сегментів буде відновлено.

- *Підтримує керування потоком* – Мережні вузли мають обмежені ресурси (зокрема, пам'ять і обчислювальну потужність). Коли TCP виявляє, що ці ресурси перевантажені, він може надіслати запит до застосунку відправника з проханням зменшити інтенсивність потоку даних. Завдяки цьому TCP регулює обсяг даних, які передає джерело. Керування потоком може запобігти необхідності повторного передавання даних, коли ресурси приймаючого вузла перебувають на межі виснаження.

Додаткові відомості про TCP можна знайти в Інтернеті у RFC 793.

Заголовок TCP

TCP – це протокол з контролем стану (stateful), який відстежує стан сеансів зв'язку. Для цього, TCP записує, яку інформацію він надіслав і яку було підтверджено. Сеанс зв'язку з контролем стану розпочинається зі встановлення сеансу обміну даними і закінчується його припиненням.

При інкапсуляції даних прикладного рівня TCP-сегмент додає 20 байтів (тобто 160 бітів) накладних витрат. На рисунку показано поля TCP-заголовку.

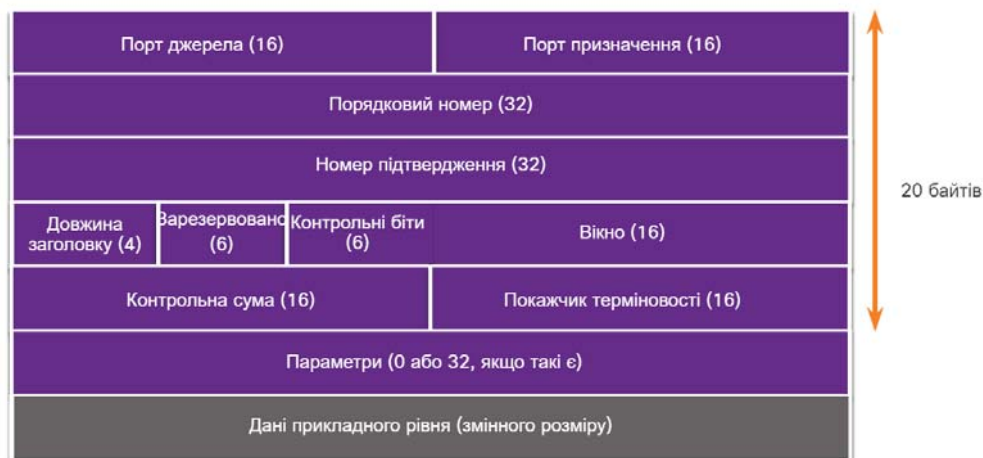


Рис. 8.6. Поля заголовка TCP

У таблиці 8.3 вказано та описано десять полів заголовка TCP.

Таблиця 8.3.

Поля заголовка TCP

<i>Поля заголовка TCP</i>	<i>Опис</i>
<i>Порт джерела</i>	16-бітне поле, яке використовується для ідентифікації застосунку відправника за номером порту.
<i>Порт призначення</i>	16-бітне поле, яке використовується для ідентифікації застосунку одержувача за номером порту.
<i>Порядковий номер (Sequence Number)</i>	32-бітне поле, яке використовується для відновлення послідовності надходження даних.
<i>Номер підтвердження (Acknowledgment Number)</i>	Поле довжиною 32 біти, яке використовується для засвідчення отримання даних, а також зазначення номера наступного байта, що очікується від джерела.
<i>Довжина заголовка (Header Length)</i>	4-бітне поле, відоме як «зсув даних», що містить довжину заголовка TCP-сегмента.
<i>Зарезервоване</i>	Поле довжиною 6 бітів, яке зарезервоване для майбутнього використання.
<i>Контрольні біти (Control bits)</i>	6-бітне поле, що містить бітові коди або прапорці, які вказують на призначення і функції сегмента TCP.
<i>Розмір вікна (Window size)</i>	16-бітне поле, яке використовується для позначення кількості байтів, які можуть бути прийняті за один раз.
<i>Контрольна сума (Checksum)</i>	Поле розміром 16 бітів, яке використовується для перевірки помилок у даних та у заголовку сегмента.
<i>Ознака терміновості (Urgent)</i>	16-бітне поле, яке використовується як ознака того, що сегмент містить термінові дані.

Застосунки, які використовують TCP

TCP є гарним прикладом того, як різні рівні стеку протоколів TCP/IP виконують визначені ролі. TCP обробляє усі завдання, пов'язані із розбиттям

поток даних на сегменти, забезпеченням надійності, керуванням потоком даних і перегрупованням сегментів. TCP звільняє застосунок від необхідності виконання будь-яких із цих функцій. Як показано на рисунку, прикладні програми можуть просто передавати потік даних на транспортний рівень і користуватися сервісами TCP.

8.3.2. Протокол користувацьких дейтаграм UDP

Протокол користувацьких дейтаграм (User Datagram Protocol, UDP) – протокол транспортного рівня, простіший за TCP. Він не забезпечує надійність і керування потоком, а отже, потребує меншої кількості полів заголовка. Через те, що відправник і отримувач UDP-процесів не повинні контролювати надійність і потоки даних, UDP-дейтаграми обробляються швидше, за TCP-сегменти. UDP забезпечує основні функції для доставки дейтаграм між відповідними застосунками, з незначними накладними витратами та перевіркою даних. UDP розділяє дані на дейтаграми, які також називаються сегментами.

UDP – це протокол без встановлення з'єднання. Оскільки UDP не забезпечує надійності або контролю за потоком даних, він не вимагає попереднього налаштування з'єднання. Оскільки UDP не відстежує інформацію, якою обмінюються клієнт і сервер, він також відомий як протокол, незалежний від стану (stateless).

UDP не гарантує доставки (best-effort), проте робить для цього все можливе, оскільки немає можливості пересвідчитись в успішному доправленні даних за призначенням. При використанні UDP відсутні процеси транспортного рівня, які інформують відправника про успішну доставку.

Робота UDP схожа на надсилання поштою звичайного, незареєстрованого листа. Відправник листа не знає, чи зможе одержувач його отримати. Крім того, поштове відділення не відповідає за відстеження листа або інформування відправника, якщо лист не надійде до кінцевого пункту призначення.

Натисніть кнопку «Відтворити» на рисунку, щоб переглянути процес передавання UDP-сегментів від відправника до одержувача.

Функції UDP

Ця тема присвячена протоколу UDP, а саме, його функціям, і рекомендаціям щодо використання замість TCP. UDP є транспортним

протоколом найкращих зусиль (best-effort). UDP – це спрощений транспортний протокол, який так само, як і TCP, виконує сегментацію і збирання даних, але без підтримки надійності та керування потоком.

UDP настільки простий, що зазвичай описується з точки зору того, що він не робить у порівнянні з TCP.

До особливостей UDP належать:

- Дані обробляються у тому порядку, в якому вони надходять.
- Будь-які втрачені сегменти повторно не надсилаються.
- Немає попереднього налаштування сеансу зв'язку.
- Відправник не інформується про доступність ресурсів з боку одержувача.

Щоб отримати додаткові відомості про UDP, можна скористатися пошуком RFC в Інтернеті.

UDP-заголовок

UDP – протокол без контролю стану (stateless), коли ані клієнт, ані сервер не відстежують стан сеансу з'єднання. Якщо при використанні UDP як транспортного протоколу все ж потрібна надійність, її повинен забезпечувати застосунок.

Однією з найважливіших вимог до трансляції відео та голосу по мережі є швидке і неперервне надходження даних. Застосунки для онлайн-трансляцій можуть допускати деяку втрату даних із мінімальним або непомітним ефектом, тому для них ідеально підходить UDP.

Блоки повідомлень протоколу UDP називають дейтаграмами або сегментами. При надсиланні дейтаграм цей транспортний протокол докладає найбільших зусиль (best-effort), виходячи зі своїх можливостей.

У порівнянні з TCP, заголовок UDP набагато простіший, оскільки містить лише чотири поля і потребує 8 байтів (тобто 64 біти). На рисунку 8.7 показано поля TCP-заголовка.



Рис. 8.7. Поля заголовка UDP

У таблиці визначено та описано чотири поля заголовка UDP.

Таблиця 8.4.

Поля заголовка UDP

Поля заголовка UDP	Опис
<i>Порт джерела</i>	16-бітне поле, яке використовується для ідентифікації застосунку відправника за номером порту.
<i>Порт призначення</i>	16-бітне поле, яке використовується для ідентифікації застосунку одержувача за номером порту.
<i>Довжина (Length)</i>	16-бітне поле, яке вказує довжину заголовка UDP-дейтаграми.
<i>Контрольна сума (Checksum)</i>	16-бітне поле, яке використовується для перевірки наявності помилок у даних і в заголовку дейтаграм.

Застосунки, які використовують UDP

Існує три типи застосунків, які найкраще підходять для UDP:

- *Мультимедійні і відео застосунки, що працюють наживо* – Ці програми допускають деякі втрати даних, але вимагають дуже невеликих затримок або повної їх відсутності. Приклади включають VoIP і потокове відео.
- *Прості застосунки типу "запит-відгук"* – Застосунки, що працюють у режимі простих транзакцій, де вузол, надсилаючи запит, може не отримати відповіді. До них належать протоколи DNS і DHCP.
- *Програми, які самі забезпечують надійність* – Однонаправлені з'єднання, які не потребують керування потоком, виявлення помилок, підтвердження про доставку та виправлення помилок, або це може забезпечити сам застосунок. Прикладами є протоколи SNMP і TFTP.

8.3.3 Порти транспортного рівня

Протоколи транспортного рівня TCP і UDP використовують номери портів для керування кількома одночасними діалогами. Як показано на

рисунку, поля заголовків TCP і UDP ідентифікують номери портів застосунків джерела й отримувача. Поля заголовка порту джерела і порту призначення мають довжину по 2 байти.

Порт джерела (16)	Порт призначення (16)

Номер порту джерела пов'язаний із вихідною програмою на локальному вузлі, тоді як номер порту отримувача пов'язаний з програмою призначення на віддаленому вузлі [8].

Наприклад, припустимо, що вузол запитує у веб-сервера деяку веб-сторінку. При цьому номер порту джерела генерується динамічно вузлом для унікальної ідентифікації цього діалогу. Кожен запит, ініційований вузлом, використовуватиме інший динамічно створений номер вихідного порту. Завдяки цьому процесу можна встановлювати кілька сеансів зв'язку одночасно.

У запиті номер порту призначення визначає тип послуги, яка вимагається від веб-сервера. Наприклад, якщо клієнт вказує 80, як порт призначення, то сервер, який отримує повідомлення, знає, що це запит веб-сервісу.

Сервер може одночасно пропонувати більше ніж одну послугу, зокрема, веб-сервіси на порті 80 і налаштування з'єднання за протоколом FTP на порті 21 для обміну файлами.

Пари сокетів

Номери портів джерела та призначення прописані у сегменті. Далі ці сегменти інкапсулюються в IP-пакети. IP-пакет містить IP-адресу джерела і призначення. Комбінацію вихідної IP-адреси та номера порту джерела, або IP-адреси та номера порту призначення, називають сокетом.

Сокети дозволяють розрізняти декілька процесів, запущених на клієнтському комп'ютері, а також розмежовувати кілька звернень до серверного процесу.

Номер порту джерела виконує роль адреси повернення для застосунку, що надіслав запит. Транспортний рівень відстежує цей порт і програму, яка ініціювала запит, щоб при надходженні можна було скерувати відповідь до потрібного застосунку.

Групи номерів портів

Адміністрація адресного простору Інтернет (Internet Assigned Numbers Authority, IANA) – це організація зі стандартизації, відповідальна за призначення різних стандартів адресації, в тому числі 16-бітних номерів портів. 16 бітів, які використовуються для ідентифікації номерів портів джерела й одержувача, забезпечують діапазон значень від 0 до 65535.

Організація IANA розбиває цей діапазон на такі три групи портів.

Таблиця 8.5.

Групи портів

<i>Група портів</i>	<i>Діапазон номерів</i>	<i>Опис</i>
<i>Відомі порти</i>	від 0 до 1023	- Ці номери портів зарезервовані для традиційних або популярних послуг і програми, таких як веб-переглядачі, поштові клієнти та клієнти віддаленого доступу. - Відомі порти, визначені для типових серверних застосунків, дозволяють клієнтам легко ідентифікувати відповідні запитувані послуги.
<i>Зареєстровані порти</i>	від 1024 до 49151	- Ці номери портів присвоюються IANA на запит суб'єкта для використання з певними процесами або програмами. - Насамперед, ці процеси пов'язані з окремими застосунками, які вирішив інсталювати користувач, а не з традиційними програмами,

<i>Група портів</i>	<i>Діапазон номерів</i>	<i>Опис</i>
		яким зазвичай надається відомий номер порту. Наприклад, Cisco зареєструвала порт 1812 для процесу автентифікації свого RADIUS-сервера.
<i>Приватні та/або Динамічні порти</i>	від 49152 до 65535	- Ці порти також відомі як <i>одноденні порти</i>. - ОС клієнта зазвичай призначає номери портів динамічно, коли ініціюється звернення до сервісу. - Далі динамічний порт використовується для ідентифікації клієнтського застосунку під час з'єднання.

Деякі клієнтські операційні системи можуть використовувати зареєстровані номери портів замість динамічних для позначення вихідних портів.

У таблиці наведені деякі відомі номери портів і традиційні застосунки, пов'язані з ними.

Таблиця 8.6.

Відомі номери портів

<i>Номер порту</i>	<i>Протокол</i>	<i>Застосунок</i>
20	TCP	Протокол передавання файлів (File Transfer Protocol, FTP) – дані
21	TCP	Протокол передавання файлів (File Transfer Protocol, FTP) – керування
22	TCP	Безпечна оболонка (Secure Shell, SSH)

<i>Номер порту</i>	<i>Протокол</i>	<i>Застосунок</i>
23	TCP	Telnet
25	TCP	Простий протокол передавання електронної пошти (Simple Mail Transfer Protocol, SMTP)
53	UDP, TCP	Служба доменних імен (Domain Name System, DNS)
67	UDP	Динамічний протокол налаштування вузла (Dynamic Host Configuration Protocol, DHCP) – сервер
68	UDP	Динамічний протокол налаштування вузла (Dynamic Host Configuration Protocol, DHCP) – клієнт
69	UDP	Простий протокол передавання файлів (Trivial File Transfer Protocol, TFTP)
80	TCP	Протокол передавання гіпертексту (Hypertext Transfer Protocol, HTTP)
110	TCP	Поштовий протокол версії 3 (Post Office Protocol v.3, POP3)
143	TCP	Протокол доступу до Інтернет-повідомлень (Internet Message Access Protocol, IMAP)
161	UDP	Простий протокол керування мережею (Simple Network Management Protocol, SNMP)
443	TCP	Захищений протокол передавання гіпертексту (Hypertext Transfer Protocol Secure, HTTPS)

Деякі програми можуть використовувати як TCP, так і UDP. Наприклад, DNS використовує UDP, коли клієнти надсилають запити до DNS-сервера. Проте, при з'єднанні між двома DNS-серверами завжди використовується TCP.

На веб-сайті IANA можна знайти реєстр з повним переліком номерів портів і пов'язаних з ними програм.

8.4. Протоколи міжмережевого рівня

Протокол IP

- *IPv4, Internet Protocol version 4* – Інтернет-протокол версії 4. Отримує повідомлення-сегменти з транспортного рівня, вкладає ці повідомлення в пакети і спрямовує сформовані пакети на рівень мережного доступу для наскрізної доставки через мережу. IPv4 використовує 32-бітні адреси.

- *IPv6, Internet Protocol version 6* – Інтернет-протокол версії 6. Схожий на IPv4, але використовує 128-бітні адреси.

- *NAT, Network Address Translation* – технологія трансляції (перетворення, заміни) мережних адрес. Замінює (транслює) приватні IP-адреси на глобальні унікальні публічні IP-адреси.

Протоколи обміну службовими повідомленнями

- *ICMPv4, Internet Control Message Protocol for IPv4* – протокол міжмережних керуючих повідомлень. Забезпечує зворотний зв'язок від вузла призначення до вихідного вузла, щоб повідомляти про помилки доставки пакетів.

- *ICMPv6, Internet Control Message Protocol for IPv6* – протокол міжмережних керуючих повідомлень для IPv6. Функціонал протоколу схожий на ICMPv4, але використовується для IPv6.

- *ICMPv6 Neighbor Discovery* – протокол виявлення сусідів. Містить чотири повідомлення протоколу ICMPv6, які використовуються для визначення адрес і виявлення адрес, що повторюються.

Протоколи маршрутизації

- *OSPF, Open Shortest Path First* – протокол знаходження найкоротшого шляху. Протокол маршрутизації з врахуванням стану каналу зв'язку, який використовує ієрархічний дизайн на основі областей. OSPF – відкритий внутрішньошлюзовий протокол маршрутизації.

- *EIGRP, Enhanced Interior Gateway Routing Protocol* – вдосконалений внутрішньо-шлюзовий протокол маршрутизації. Власний протокол маршрутизації Cisco, що використовує комплексну метрику, до якої входять пропускна здатність, затримка, навантаження та надійність.

- *BGP, Border Gateway Protocol* – протокол граничного шлюзу. Відкритий зовнішньошлюзовий протокол маршрутизації, що використовується для передавання даних між постачальниками послуг Інтернету (ISP, Internet Service Providers). BGP також використовується для обміну маршрутною інформацією між Інтернет-провайдерами та їх великими приватними клієнтами.

8.4.1 Протокол IP

IP-протокол – найпоширеніша реалізація ієрархічної схеми мережевої адресації. Використовуваний в мережі Інтернет, протокол відповідає за адресацію пакетів, але не відповідає за встановлення з'єднань, не є надійним і дозволяє реалізувати тільки негарантовану доставку даних. Термін «протокол без встановлення з'єднань» (англ. connectionless) означає, що протокол для взаємодії не потребує виділеного каналу, як це відбувається під час телефонної розмови і не існує процедури виклику перед початком передачі даних між мережевими вузлами. Протокол IP вибирає найефективніший шлях з числа доступних на основі рішень прийнятих протоколом маршрутизації. Відсутність надійності і негарантована доставка не означає, що система працює погано або ненадійно, а вказує лиш на те, що протокол IP не докладатиме ніяких зусиль, щоб перевірити чи був пакет доставлений за призначенням. Ці функції делеговані протоколам транспортного та вищих рівнів. Транспортний рівень також відповідає за збірку пакетів у повідомлення в потрібній послідовності.

Інформація, проходячи вниз по рівням моделі OSI, на кожному рівні певним чином обробляється протоколами цього рівня. На мережному рівні дані інкапсулюються всередину пакетів, іноді названих дейтаграммами (датаграммами).

Протокол IP розпізнає формат заголовка пакета (адресну частину та іншу службову інформацію включно), але не аналізує і не піклується про фактичні дані. Він приймає і передає будь-які дані, передані протоколами верхніх рівнів.

8.4.2 Протокол ICMP

Повідомлення ICMPv4 і ICMPv6

Незважаючи на те, що IP – це лише протокол з негарантованою доставкою, протокол TCP/IP надає повідомлення про помилки та

інформаційні повідомлення під час взаємодії з іншим IP-пристроєм. Ці повідомлення надсилаються за допомогою служб протоколу ICMP. Метою цих повідомлень є забезпечення зворотного зв'язку щодо питань, пов'язаних з обробкою IP-пакетів за певних умов, але не мають мети забезпечити надійність IP. Повідомлення ICMP не є обов'язковими та часто заборонені в межах мережі з міркувань безпеки.

Протокол ICMP використовується для обох протоколів, як для IPv4 так і для IPv6. ICMPv4 – це протокол обміну повідомленнями для IPv4. ICMPv6 надає ті самі служби для IPv6, але включає додаткові функціональні можливості. У цьому курсі термін ICMP буде стосуватися і ICMPv4, і ICMPv6.

Типи ICMP-повідомлень та причини їх надсилання дуже різноманітні. Повідомлення ICMP, спільні для ICMPv4 та ICMPv6 та обговорюються в цьому розділі, включають:

- Досяжність вузла
- Пункт призначення або служби недоступні
- Перевищено час очікування

Повідомлення ICMPv6

Інформаційні повідомлення та повідомлення про помилки, які виникають в ICMPv6 дуже схожі на повідомлення про контроль та помилки, реалізовані в ICMPv4. Однак ICMPv6 має нові можливості та вдосконалену функціональність, які не можна знайти в ICMPv4. Повідомлення ICMPv6 інкапсулюються в IPv6.

Протокол ICMPv6 включає в себе чотири нових протоколи, що входять до складу протоколу виявлення сусідів (ND або NDP, Neighbor Discovery Protocol).

Обмін повідомленнями між маршрутизатором IPv6 і пристроєм IPv6, включаючи динамічний розподіл адрес, здійснюється за допомогою повідомлень:

- Запит маршрутизатора (RS, Router Solicitation)
- Анонсування маршрутизатора (RA, Router Advertisement)

Обмін повідомленнями між пристроями IPv6, включаючи виявлення дублікатів адреси та визначення адреси, здійснюється за допомогою повідомлень:

- Запит сусіда (NS, Neighbor Solicitation)
- Анонсування сусіда (NA, Neighbor Advertisement)

ICMPv6 ND також включає в себе перенаправлення повідомлення, яке має функцію, схожу на подібну функцію перенаправлення повідомлення, що використовується в ICMPv4.

8.5. Рівень мережного доступу

Визначення адрес

- *ARP, Address Resolution Protocol* – протокол визначення адрес. Забезпечує динамічне співставлення IPv4-адресою та апаратною адресою.

Протоколи канального рівня

- *Ethernet* – визначає правила для стандартів кабельної інфраструктури та стандартів передачі сигналів на рівні мережного доступу.
- *WLAN, Wireless Local Area Network* – бездротова локальна мережа. Визначає правила бездротової передачі сигналів на радіочастотах 2,4 ГГц і 5 ГГц.

8.5.1. Протокол ARP

Для визначення локальної адреси за IP-адресою використовується протокол вирішення адрес (Address Resolution Protocol, ARP). ARP реалізується по-різному залежно від того, чи працює він у локальній мережі (Ethernet, Wi-Fi) з можливістю ширококомовлення, або ж у глобальній мережі (MPLS, ATM), які зазвичай не підтримують ширококомовний доступ.

Протокол ARP підтримує на кожному інтерфейсі мережевого адаптера або маршрутизатора окрему ARP-таблицю, у якій під час функціонування мережі накопичується інформація про відповідність між IP-адресами та MAC-адресами інших інтерфейсів даної мережі. Спочатку, під час увімкнення комп'ютера або маршрутизатора в мережу, всі його ARP-таблиці порожні.

1. На першому кроці відбувається передача від протоколу IP протоколу ARP приблизно такого повідомлення: "Яку MAC-адресу має інтерфейс з адресою IP?"

2. Робота протоколу ARP починається з перегляду власної ARP-таблиці. Припустимо, що серед записів, які містяться в ній, відсутня запитувана IP-адреса.

3. У цьому випадку протокол ARP формує ARP-запит, вкладає його в кадр протоколу Ethernet і робить ширококомовну розсилку. Зауважимо, що зона

поширення ARP-запиту обмежується мережею Ethernet, оскільки на шляху широкомовних кадрів бар'єром стоїть маршрутизатор.

4. Усі інтерфейси мережі Ethernet отримують ARP-запит і направляють його "своєму" протоколу ARP. ARP порівнює зазначену в запиті адресу IP з IP-адресою власного інтерфейсу.

5. Протокол ARP, який констатував збіг, формує ARP-відповідь, у якій маршрутизатор вказує локальну MAC-адресу, що відповідає адресі IP свого інтерфейсу, і відправляє її вузлу, що запитує.

Щоб зменшити кількість ARP-звернень, запис про знайдену відповідність між IP-адресою і MAC-адресою зберігається в ARP-таблиці відповідного інтерфейсу. Цей запис в ARP-таблиці з'являється автоматично, через кілька мілісекунд після того, як модуль ARP проаналізує ARP-відповідь.

Протокол ARP, отримавши запит, насамперед переглядає свою ARP-таблицю і робить широкомовний запит тільки в тому разі, якщо в таблиці немає запису про запитану адресу. ARP-таблиця поповнюється не тільки за рахунок ARP-відповідей, що надходять на даний інтерфейс ARP-відповідей, а й у результаті вилучення корисної інформації з широкомовних ARP-запитів. Усі інтерфейси, які отримали цей запит, можуть помістити інформацію про відповідність локальної та мережевої адрес відправника у власну ARP-таблицю

В ARP-таблицях існують два типи записів: динамічні та статичні. Статичні записи створюються вручну за допомогою утиліти ARP і не мають терміну старіння, точніше, вони існують доти, доки комп'ютер або маршрутизатор залишається увімкненим.

Динамічні записи повинні періодично оновлюватися. Якщо запис не оновлювався 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 беруть активну участь у мережевих операціях. Оскільки такий спосіб зберігання інформації називають кешуванням, ARP-таблиці іноді називають ARP-кешем [2].

Контрольні запитання

1. Що таке стек протоколів і чому він важливий для функціонування мережі?

2. Що означає відкритий стандартний набір протоколів у випадку TCP/IP?
3. Які протоколи входять в стек TCP/IP, і які їхні основні функції?
4. Що робить протокол DNS (Domain Name System) і яка його роль у мережах?
5. Які протоколи використовуються для налаштування мережеских вузлів в IPv4 та IPv6?
6. Що таке автоматичне налаштування адреси без відстеження стану (SLAAC)?
7. Назвіть протоколи електронної пошти, їхні функції та різницю між ними.
8. Які протоколи використовуються для передавання файлів у мережі і яка їхня основна призначеність?
9. Що таке протокол HTTPS і чому він важливий для безпеки передачі даних в мережі?
10. Які основні типи ресурсних записів DNS і для чого вони використовуються?
11. Яким чином працює протокол DHCP (Dynamic Host Configuration Protocol) для надання IP-адрес та інших параметрів клієнтам у мережі?
12. Які основні типи повідомлень в протоколі HTTP і що вони використовуються для?
13. Що робить протокол SFTP (Secure Shell FTP) і як він відрізняється від звичайного FTP?
14. Які основні методи HTTP-запитів і що вони використовуються для?
15. Що відповідає за структуру, адресацію та маршрутизацію пакетів на транспортному рівні TCP/IP?
16. Які основні завдання транспортного рівня стека TCP/IP?
17. Які два протоколи транспортного рівня використовуються в TCP/IP, і які їх відмінності?
18. Які послуги надає TCP в рамках транспортного рівня?
19. Які функції виконує UDP на транспортному рівні, і як він відрізняється від TCP?
20. Що таке порти транспортного рівня, і як вони використовуються в TCP і UDP?
21. Як організація IANA розподіляє номери портів і які групи портів існують?

22. Що таке NAT (Network Address Translation), і як він використовується в мережах?

23. Які протоколи обміну службовими повідомленнями використовуються в мережевому стеку?

24. Які функції виконує протокол ICMP (Internet Control Message Protocol)? Для чого використовуються ICMPv4 і ICMPv6?

25. Які повідомлення входять до складу протоколу ICMPv6 Neighbor Discovery і як вони використовуються?

26. Що таке ARP (Address Resolution Protocol), і як він допомагає визначати локальну адресу за IP-адресою?

27. Які протоколи канального рівня згадуються в тексті? Для чого вони використовуються?

28. Які типи записів існують в ARP-таблицях, і яка їх відмінність між собою?

РОЗДІЛ 9. ГЛОБАЛЬНІ КОМП'ЮТЕРНІ МЕРЕЖІ

9.1. Основні поняття і визначення.

Загальна структура й функції глобальних мереж

Глобальна мережа (wide area network, WAN) охоплює значну географічну область, цілу країну або навіть континент. Вона поєднує машини, які призначені для виконання програм користувача (тобто прикладних програм). Хости (машини користувача) з'єднуються комунікаційними підмережами, які називають для стислості підмережами. Хости звичайно є власністю клієнтів (тобто просто клієнтськими комп'ютерами), у той час як комунікаційною підмережею найчастіше володіє та управляє телефонна компанія або постачальник послуг Інтернету. Завданням підмережі є передача повідомлень від хоста до хосту, подібно тому, як телефонна система переносить слова від розмовляючого до слухача. Таким чином, комунікативний аспект мережі (підмережі) відділений від прикладного аспекту (хостів), що значно спрощує структуру мережі.

У більшості глобальних мереж підмережа складається із двох роздільних компонентів: ліній зв'язку й перемикаючих елементів. Лінії зв'язку, які називаються каналами або магістралями, переносять дані від машини до машини. Перемикаючі елементи є спеціалізованими комп'ютерами, що використовуються для з'єднання трьох або більше ліній зв'язку. Коли дані з'являються на вхідній лінії, перемикаючий елемент має вибрати вихідну лінію – подальший маршрут цих даних. У минулому для назви цих комп'ютерів не було стандартної термінології. Зараз їх називають маршрутизаторами (router).

У моделі, яка наведена на рис.9.1, кожний хост з'єднаний з локальною мережею, у якій присутній маршрутизатор, хоча в деяких випадках хост може бути пов'язаний з маршрутизатором безпосередньо. Набір ліній зв'язку і маршрутизаторів (але не хостів) створює підмережу.

Більшість глобальних мереж містять велику кількість кабелів або телефонних ліній, що з'єднують пари маршрутизаторів. Якщо які-небудь два маршрутизатори не зв'язані лінією зв'язку безпосередньо, то вони мають спілкуватися за допомогою інших маршрутизаторів. Коли пакет посилається від одного маршрутизатора до іншого через декілька проміжних маршрутизаторів, він отримується кожним проміжним маршрутизатором цілком, зберігається на ньому, поки необхідна лінія зв'язку не звільниться, а потім пересилається далі. Підмережа, що працює за таким принципом,

називається підмережею із проміжним зберіганням (store-and-forward) або підмережею з комутацією пакетів (packet-switched). Майже у всіх глобальних мережах (крім мереж, що використовують супутники зв'язку) є підмережі із проміжним зберіганням. Невеликі пакети фіксованого розміру часто називають комірками (cell).

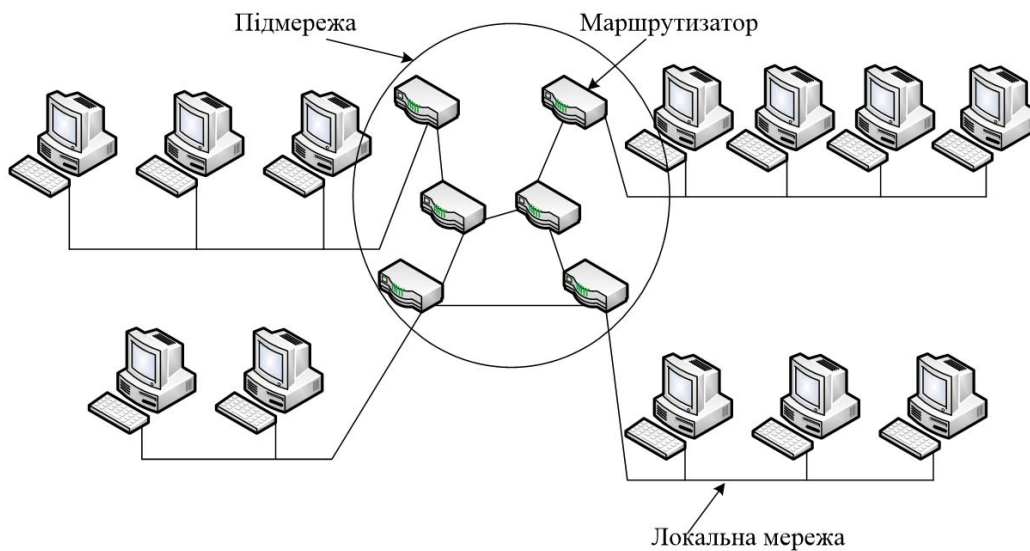


Рис. 9.1. Зв'язок хостів і підмережі у локальній мережі

Коли у процесі якого-небудь хосту з'являється повідомлення, яке він збирається відправити процесу іншого хоста, хост, який відправляє, розбиває послідовність на пакети, кожен з яких має свій порядковий номер. Пакети один за іншим направляються в лінію зв'язку і окремо передаються по мережі. Приймаючий хост збирає пакети у вихідне повідомлення і передає процесу. Просування потоку пакетів схематично показано на рис. 9.2.

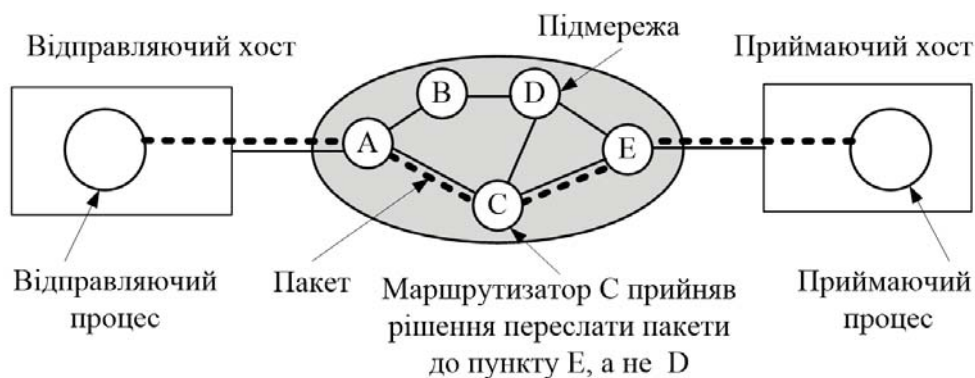


Рис. 9.2. Потік пакетів від відправляючого хоста до приймаючого

З рис.9.2 видно, що всі пакети прямують шляхом ACE, а не ABDE або ACDE. У деяких мережах шлях всіх пакетів даного повідомлення взагалі є строго визначеним. В інших мережах шлях пакетів може прокладатися незалежно.

Рішення про вибір маршруту приймається на локальному рівні. Коли пакет приходить на маршрутизатор А, саме останній вирішує, куди його перенаправляти – на В або на С. Метод ухвалення рішення називається *алгоритмом маршрутизації*.

Не всі глобальні мережі використовують комутацію пакетів. Другою можливістю з'єднати маршрутизаторів глобальної мережі є радіозв'язок з використанням супутників. Кожний маршрутизатор забезпечується антеною, за допомогою якої він може приймати й посылати сигнал. Всі маршрутизатори можуть приймати сигнали із супутника, а в деяких випадках вони можуть також чути передачі сусідніх маршрутизаторів, що передають дані на супутник. Іноді всі маршрутизатори з'єднуються звичайною підмережою, і тільки деякі з них забезпечені супутниковою антеною. Супутникові мережі є широкомовними та найбільш корисні там, де потрібне широкомовлення [9].

9.2. Глобальний зв'язок на основі виділених ліній

9.2.1 Цифрові виділені лінії

Технологія плезіохронної цифрової ієрархії PDH. Початок технології PDH було покладено розробкою мультиплексора Т-1, що дозволяв у цифровому виді мультиплексувати, передавати й комутувати (на постійній основі) голосовий трафік 24 абонентів. Тому що абоненти як і раніше користувалися звичайними телефонними апаратами, тобто передача голосу йшла в аналоговій формі, мультиплексори Т-1 самі здійснювали оцифровування голосу із частотою 8000 Гц і кодували голос методом імпульсно-кової модуляції. В результаті кожний абонентський канал створював цифровий потік даних 64 Кбіт/с, а мультиплексор Т-1 забезпечував передачу 1,544 Мбіт/с.

Для з'єднання великих телефонних станцій канали Т-1 являли собою занадто слабкі й негнучкі засоби мультиплексування, тому була реалізована ідея створення каналів з *ієрархією швидкостей*. Чотири канали типу Т-1 об'єднали в канал наступного рівня цифрової ієрархії – Т-2, що передає дані зі швидкістю 6,312 Мбіт/с. Канал Т-3, створений шляхом об'єднання семи каналів Т-2, має

швидкість 44,736 Мбіт/с. Канал Т-4 поєднує 6 каналів Т-3, у результаті його швидкість дорівнює 274 Мбіт/с. Ця технологія одержала назву системи Т-каналів.

Із середини 70-х років виділені канали, що побудовані на основі систем Т-каналів, стали здаватися телефонними компаніями в оренду на комерційних умовах, переставши бути внутрішньою технологією цих компаній. Системи Т-каналів дозволяють передавати не тільки голос, але й будь-які дані, що представлені в цифровій формі, – комп'ютерні дані, телевізійне зображення, факси та інше.

Технологія систем Т-каналів була стандартизована Американським національним інститутом стандартів (ANSI), а пізніше – міжнародним комітетом ССІТТ. При стандартизації вона одержала назву Plesiochronous Digital Hierarchy (PDH). В результаті внесених комітетом ССІТТ змін виникла несумісність американської та міжнародної версій стандарту PDH. Аналогом систем Т-каналів у міжнародному стандарті є канали типу Е-1, Е-2 і Е-3 зі швидкостями, що відрізняються, – відповідно 2,048 Мбіт/с, 8,488 Мбіт/с і 34,368 Мбіт/с. Американська версія сьогодні крім США поширена також у Канаді і Японії (з деякими розходженнями), а в Європі застосовується міжнародний стандарт ССІТТ.

Незважаючи на розходження в американській і міжнародній версіях, технології цифрової ієрархії використовують ті самі позначення для ієрархії швидкостей – DSn (Digital Signal n). У табл. 9.1 наведені значення для всіх введених стандартами рівнів швидкостей обох технологій.

Таблиця 9.1.

Ієрархія цифрових швидкостей

Позначення швидкості	США			ССІТТ (Європа)		
	Кількість голосових каналів	Кількість каналів попереднього рівня	Швидкість Мбіт/с	Кількість голосових каналів	Кількість каналів попереднього рівня	Швидкість Мбіт/с
DS-0	1	1	64 Кбіт/с	1	1	64 Кбіт/с
DS-1	24	24	1,54	30	30	2,048
DS-2	96	4	6,312	120	4	8,488
DS-3	672	7	44,736	480	4	34,368
DS-4	4032	6	274,176	1920	4	139,264

На практиці взагалі використовуються канали T1/E1 і T3/E3. Як американський, так і міжнародний варіанти технології PDH мають недоліки, основним з яких є складність і неефективність операцій мультиплексування й демуплексування даних користувачів. Сам термін “плезіохронний”, тобто “майже синхронний”, що використовується для цієї технології, говорить про причину такого явища – відсутності повної синхронності потоків даних при об’єднанні низькошвидкісних каналів у високошвидкісні. Асинхронний підхід при передачі кадрів зробив необхідною вставку біта або декількох бітів синхронізації між кадрами. В результаті для отримання користувацьких даних з об’єданого каналу необхідно повністю демуплексувати кадри об’єданого каналу. Наприклад, щоб одержати дані одного абонентського каналу 64 Кбіт/с із кадрів каналу T3, необхідно зробити демуплексування цих кадрів до рівня кадрів T2, потім – до рівня кадрів T1, а, зрештою, демуплексувати і самі кадри T1.

Якщо мережа PDH використовується тільки як транзитна магістраль між двома великими вузлами, то операції мультиплексування і демуплексування виконуються винятково в прикінцевих вузлах, і проблем не виникає. Але якщо необхідно виділити один або декілька абонентських каналів у проміжному вузлі мережі PDH, то це завдання простого рішення не має. Як варіант пропонується установка двох мультиплексорів рівня T3/E3 і вище в кожному вузлі мережі (рис.9.3). Перший виконує повне демуплексування потоку й виведення частини низькошвидкісних каналів абонентам, а другий знову збирає у вихідний високошвидкісний потік канали, що залишилися, разом із каналами, що знову вводяться. При цьому кількість працюючого обладнання подвоюється.

Інший варіант – “зворотна доставка”. У проміжному вузлі, де потрібно виділити й відвести абонентський потік, встановлюється єдиний високошвидкісний мультиплексор, що просто передає дані транзитом далі по мережі без їх демуплексування. Цю операцію виконує тільки мультиплексор прикінцевого вузла, після чого дані відповідного абонента вертаються по окремій лінії зв’язку на проміжний вузол. Зазвичай, такі складні взаємини комутаторів ускладнюють роботу мережі, вимагають її тонкого конфігурування, що веде до великого обсягу ручної роботи з помилкам. Крім цього, у технології PDH не передбачені вбудовані засоби забезпечення відмовостійкості та адміністрування мережі[8; 17; 26].

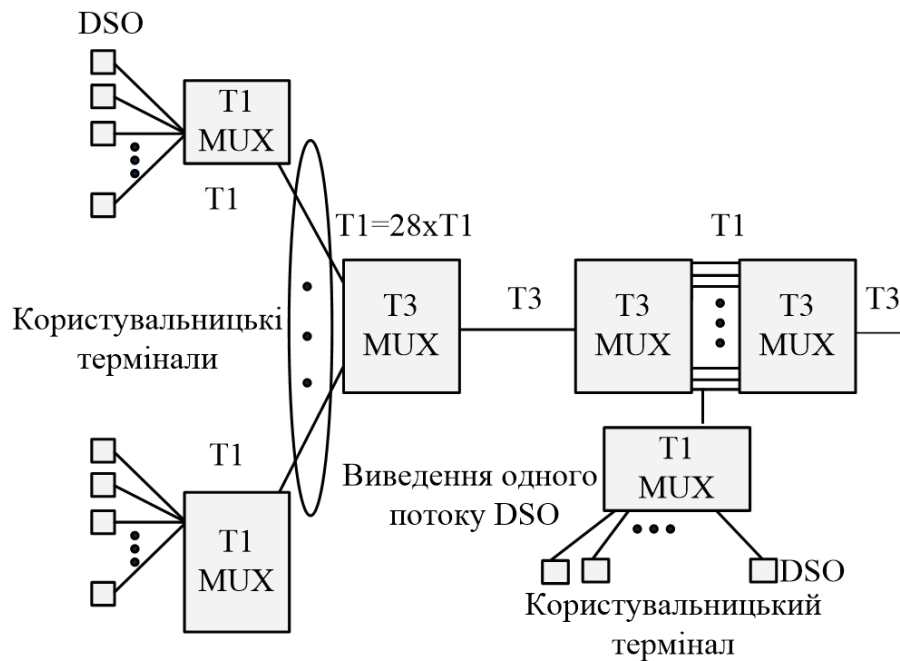


Рис. 9.3. Виділення низькошвидкісного каналу шляхом повного демультимплексування

Також недоліком PDH є занадто низькі за сучасними поняттями швидкості передачі даних. Волоконно-оптичні кабелі дозволяють передавати дані зі швидкостями в декілька гігабіт за секунду по одному волокну, що забезпечує консолідацію в одному кабелі десятків тисяч користувальницьких каналів, але цю можливість технологія PDH не реалізує – її ієрархія швидкостей закінчується рівнем 139 Мбіт/с.

Технологія синхронної цифрової ієрархії SONET/SDH

Зазначені вище недоліки були враховані й подолані розроблювачами технології синхронних оптичних мереж (Synchronous Optical NET, SONET), перший варіант стандарту якої з'явився в 1984 році. Потім вона була стандартизована комітетом T-1 інституту ANSI. Міжнародна стандартизація технології проходила під егідою Європейського інституту телекомунікаційних стандартів (European Telecommunications Standards Institute, ETSI) і сектором телекомунікаційної стандартизації союзу ITU (ITU Telecommunication Standardization Sector, ITU-T) разом з ANSI і провідними телекомунікаційними компаніями Америки, Європи і Японії. Основною метою розроблювачів міжнародного стандарту було створення технології, здатної передавати трафік всіх існуючих цифрових каналів рівня PDH (як американських DS1-DS4, так і європейських E1-E4) по високошвидкісній магістральній мережі

на базі волоконно-оптичних кабелів і забезпечити ієрархію швидкостей, що продовжує ієрархію технології PDH до швидкості в декілька гігабіт за секунду.

В результаті тривалої роботи ITU-T і ETSI вдалося розробити міжнародний стандарт SDH (Synchronous Digital Hierarchy – синхронна цифрова ієрархія). Крім того, стандарт SONET був дороблений так, щоб апаратура й мережі SDH і SONET були сумісними й могли мультиплексувати вхідні потоки практично будь-якого стандарту PDH – і американського, і європейського. Ієрархія швидкостей, що підтримана технологією SONET/SDH, наведена в табл. 9.2.

У стандарті SDH всі рівні швидкостей (формати кадрів для цих рівнів) мають загальну назву STM-N (Synchronous Transport Module level N – синхронний транспортний модуль рівня N). У технології SONET існує два позначення для рівнів швидкостей: STS-N (Synchronous Transport Signal level N – синхронний транспортний сигнал рівня N), що вживається у випадку передачі даних електричним сигналом, і OC-N (Optical Carrier level N – оптоволоконна лінія зв'язку рівня N), що вживається у випадку передачі даних по волоконно-оптичному кабелю.

Таблиця 9.2

Ієрархія швидкостей SONET/SDH

SDH	SONET	Швидкість
	STS-1, OC-1	51,84 Мбіт/с
STM-1	STS-3, OC-3	155,520 Мбіт/с
STM-3	OC-9	466,560 Мбіт/с
STM-4	OC-12	622,080 Мбіт/с
STM-6	OC-18	933,120 Мбіт/с
STM-8	OC-24	1,244 Гбіт/с
STM-12	OC-36	1,866 Гбіт/с
STM-16	OC-48	2,488 Гбіт/с
STM-64	OC-192	9,953 Гбіт/с
STM-256	OC-768	39,81 Гбіт/с

Кадри STM-N мають структуру, що дозволяє агрегувати у загальний магістральний потік потоки SDH і PDH різних швидкостей, а також виконувати операції введення-виведення без повного демультимплексування магістрального потоку.

Операції мультиплексування й введення-виведення виконуються за допомогою віртуальних контейнерів (Virtual Container, VC), у яких блоки даних PDH можна транспортувати через мережу SDH. Крім блоків даних

PDH у віртуальний контейнер розміщується ще деяка службова інформація, зокрема заголовок шляху (Path OverHead, POH) контейнера, у якому розміщується статистична інформація про процес проходження контейнера уздовж шляху від його початкового до прикінцевого пункту (повідомлення про помилки), а також інші службові дані (індикатор встановлення з'єднання між прикінцевими пунктами). В результаті розмір віртуального контейнера виявляється більше, ніж відповідне навантаження у вигляді блоків даних PDH, що він переносить.

У технології SDH (рис.9.4) визначено декілька типів віртуальних контейнерів, призначених для транспортування основних типів блоків даних PDH: VC-11 (1,5 Мбіт/с), VC-12 (2 Мбіт/с), VC-2 (6 Мбіт/с), VC-3 (34/45 Мбіт/с) і VC-4 (140 Мбіт/с).

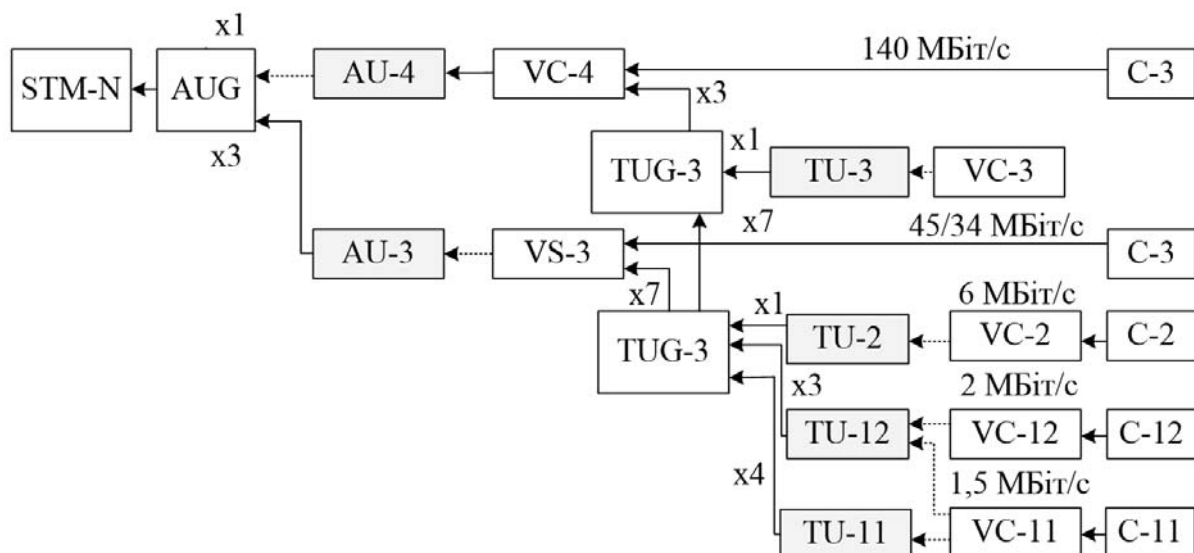


Рис. 9.4. Схема мультиплексування даних в SDH

Віртуальні контейнери є *одиницею комутації* мультиплексорів SDH. У кожному мультиплексорі існує таблиця з'єднань (що називається також таблицею кросів-з'єднань), у якій зазначено, наприклад, що контейнер VC-12 порту P1 з'єднаний з контейнером VC-12 порту P5, а контейнер VC-3 порту P8 – з контейнером VC-3 порту P9. Таблицю з'єднань формує адміністратор мережі за допомогою системи керування або керуючого термінала на кожному мультиплексорі так, щоб забезпечити наскрізний шлях між прикінцевими пунктами мережі, до яких підключене користувальницьке обладнання.

Для з'єднання в рамках однієї мережі механізмів синхронної передачі кадрів (STM-N) з асинхронним характером користувальницьких даних PDH у

технології SDH, що переносяться цими кадрами, застосовуються показчики. *Концепція показчиків* – ключова в технології SDH, вона заміняє прийняте в PDH вирівнювання швидкостей асинхронних джерел за допомогою додаткових бітів. Показчик визначає поточне положення віртуального контейнера в агрегованій структурі більш високого рівня – трибутарному блоці (Tributary Unit, TU) або адміністративному блоці (Administrative Unit, AU). Основна відмінність цих блоків від віртуального контейнера полягає в наявності додаткового поля показчика. За допомогою цього показчика віртуальний контейнер може “зміщуватися” у певних межах усередині свого трибутарного або адміністративного блоку, положення якого, у свою чергу, у кадрі фіксовано. Завдяки системі показчиків мультиплексор знаходить положення користуvalницьких даних у синхронному потоці байтів кадрів STM-N і витягує їх звідти, чого механізм мультиплексування, що застосовується в PDH, робити не дозволяє.

Трибутарні блоки поєднуються в групи, а вони входять в адміністративні блоки. Група з N адміністративних блоків (Administrative Unit Group, AUG) і утворює корисне навантаження кадру STM-N. Крім цього в кадрі є заголовок із загальною для всіх блоків AU службовою інформацією. На кожному кроці перетворення до попередніх даних додається декілька службових байтів: вони допомагають розпізнати структуру блоку або групи блоків і потім визначити за допомогою показчиків початок користуvalницьких даних.

На рис. 9.5 структурні одиниці кадру SDH, що містять показчики, заштриховані, а зв’язок між контейнерами й блоками, що допускає зсув даних за фазою, вказано пунктиром. Схема мультиплексування SDH надає різноманітні можливості по об’єднанню користуvalницьких потоків PDH. Наприклад, для кадру STM-1 можна реалізувати такі варіанти:

- 1 потік E-4;
- 63 потоки E-1;
- 1 потік E-3 і 42 потоки E-1 і т.д.

Основним елементом мережі SDH є мультиплексор (рис. 9.5). Він оснащений деякою кількістю портів PDH і SDH. Порти мультиплексора SDH діляться на агрегатні (лінійні порти) і трибутарні (порти введення-виведення).

Мультиплексори SDH розділяють на два типи: термінальний мультиплексор і мультиплексор введення-виведення. Термінальний мультиплексор (Terminal Multiplexer, TM) завершує агрегатні канали, мультиплексуючи в них велику кількість трибутарних каналів. Термінальний

мультиплексор оснащений одним агрегатним портом і великою кількістю трибутарних портів (рис. 9.6).

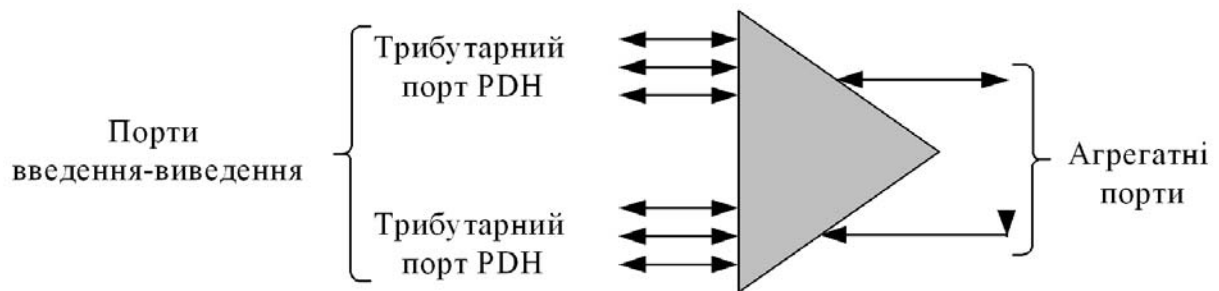


Рис. 9.5. Мультиплексор SDH

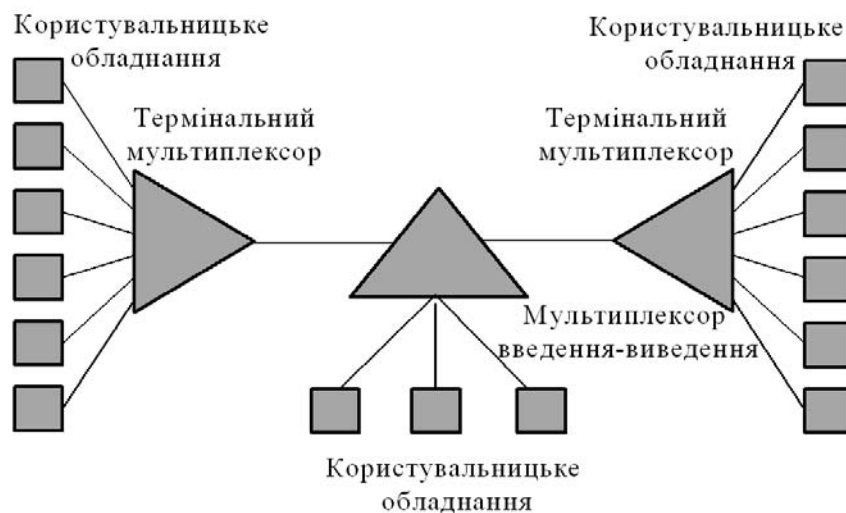


Рис. 9.6. Типи мультиплексорів SDH

Мультиплексор введення-виведення (Add-Drop Multiplexer, ADM) займає проміжне положення на магістралі (у кільці, ланцюзі або змішаній топології). Він має два агрегатних порти, транзитом передаючи агрегатний потік даних. За допомогою невеликої кількості трибутарних портів такий мультиплексор вводить в агрегатний потік або виводить із агрегатного потоку дані трибутарних каналів.

Розрізняють також *цифрові кросс-конектори* (Digital Cross-Connect, DCC) – мультиплексори, які виконують операції комутації над довільними віртуальними контейнерами. У таких мультиплексорах не має відмінностей між агрегатними й трибутарними портами, тому що вони призначені для роботи в комірчастій топології, де неможливо виділити агрегатні потоки.

Крім мультиплексорів до складу мережі SDH можуть входити регенератори сигналів, що необхідні для подолання обмежень за відстанню між мультиплексорами. Ці обмеження залежать від потужності оптичних передавачів, чутливості приймачів і згасання волоконно-оптичного кабелю. Регенератор перетворює оптичний сигнал в електричний і назад, при цьому відновлюється форма сигналу і його часові характеристики. В той же час регенератори SDH застосовуються досить рідко, тому що вартість їх ненабагато менша вартості мультиплексора, а функціональні можливості менші.

Стек протоколів SDH. Стек протоколів складається із протоколів 4-х рівнів. Вони ніяк не співвідносяться з рівнями моделі OSI, для якої вся мережа SDH являє собою обладнання фізичного рівня. Фотонний рівень здійснює кодування бітів інформації шляхом модуляції світла. Для кодування оптичного сигналу застосовується потенційний код NRZ, що володіє властивостями самосинхронізації.

Рівень секції підтримує фізичну цілісність мережі. *Регенераторною секцією* в технології SDH називається кожний безперервний відрізок волоконно-оптичного кабелю, що з'єднує між собою, наприклад, такі пари пристроїв SONET/SDH, як мультиплексор і регенератор, регенератор і регенератор (але не два мультиплексора). Компоненти регенераторної секції підтримують протокол, що має справу з певною частиною заголовка кадру (заголовком регенераторної секції Regenerator Section OverHead, RSOH), на основі службової інформації може проводити тестування секції й виконувати операції адміністративного контролю.

Рівень лінії відповідає за передачу даних по лінії між двома мультиплексорами мережі, тому лінію також часто називають мультиплексною секцією. Протокол цього рівня працює з кадрами рівнів STS-N для виконання різних операцій мультиплексування й демультиплексування, а також вставки й видалення користувальницьких даних. Протокол лінії також відповідає за реконфігурування лінії у випадку відмови якого-небудь її елемента – оптичного волокна, порту або сусіднього мультиплексора. Службова інформація мультиплексної секції розташовується в частині заголовка кадру, яка називається заголовком мультиплексної секції (Multiplex Section OverHead, MSOH).

Рівень тракту відповідає за доставку даних між двома прикінцевими користувачами мережі. *Тракт* – це складене віртуальне з'єднання між користувачами. Протокол тракту повинен прийняти дані, що надходять у

користувальницькому форматі, наприклад форматі T1, і перетворити їх у синхронні кадри STM-N.

Основні елементи кадру STM-1 показані на рис. 9.7, а у табл. 9.3 наведена структура заголовків регенераторної й мультимплексної секцій. Кадр звичайно представляють у вигляді матриці, що складається з 270 стовпців і 9 рядків. Перші 9 байт кожного рядка відводяться під службові дані заголовків, з наступних 261 байт 260 відводяться під корисне навантаження (дані таких структур, як AUG, AU, TUG, TU і VC), а один байт кожного рядка приділяється під заголовок тракту, що дозволяє контролювати з'єднання “від краю до краю”.

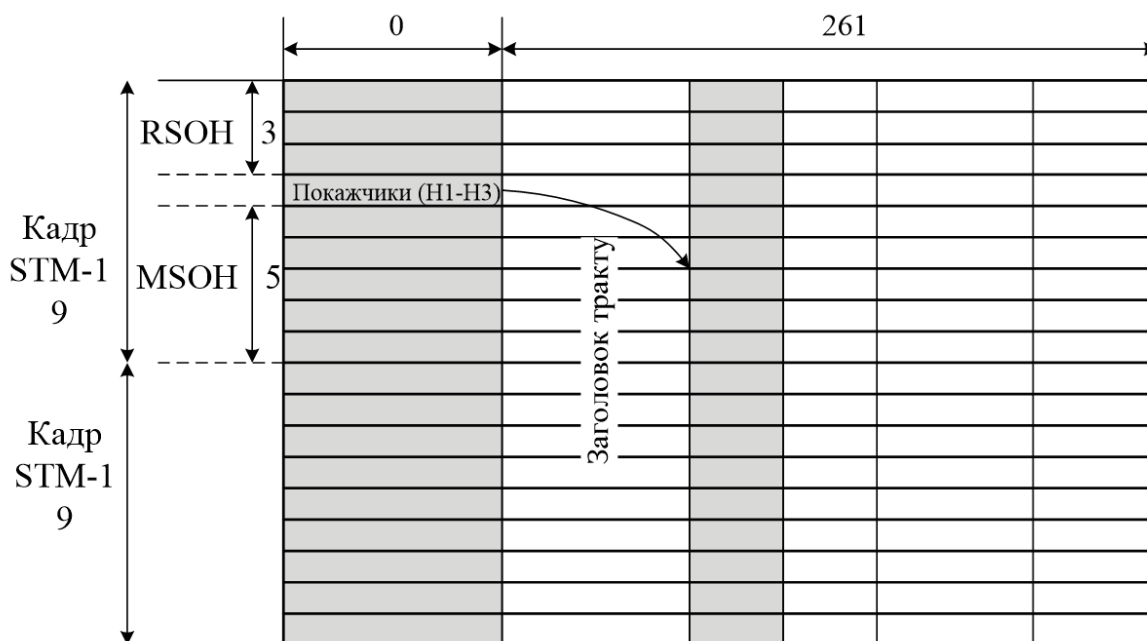


Рис. 9.7. Структура кадру STM-1

Механізм роботи показника H1-H2-H3 найбільш зручно розглянути на прикладі кадру STM-1, що переносить контейнер VC-4. Показник займає 9 байт четвертого ряду кадру, під кожне з полів H1, H2 і H3 приділяється по 3 байти. Дозволені значення показника перебувають у діапазоні 0-782, показник відзначає початок контейнера VC-4 у трибайтових одиницях. Фіксоване значення показника дозволяє врахувати фазовий зсув між даним мультимплексором і джерелом даних, у якості якого може виступати мультимплексор PDH, обладнання користувача з інтерфейсом PDH або інший мультимплексор SDH. В результаті віртуальний контейнер передається у двох послідовних кадрах STM-1.

Показник може відпрацьовувати не тільки фіксований фазовий зсув, але й неузгодженість тактової частоти мультимплексора з тактовою частотою

пристрою, від якого приймаються користувальницькі дані. Для компенсації цього ефекту значення показчика періодично збільшується або зменшується на одиницю. Якщо швидкість надходження даних контейнера VC-4 менше, ніж швидкість відправлення STM-1, то у мультиплексорі періодично (цей період залежить від величини неузгодженості частоти синхронізації) виникає недостача користувальницьких даних для заповнення відповідних полів віртуального контейнера.

Таблиця 9.3

Структура заголовків регенераторної та мультиплексної секцій

Заголовок регенераторної секції	Заголовок мультиплексної секції
Синхробайти	Байти контролю помилок для мультиплексної секції
Байти контролю помилок для регенераторної секції	Шість байтів каналу передачі даних, що працюють зі швидкістю 576 Кбіт/с
Один байт службового аудіоканалу	Два байти протоколу автоматичного захисту трафіку (байти K1 та K2), що забезпечують живучість мережі
Три байти каналу передачі даних (Data Communications Channel, DCC), що працюють із швидкістю 192 Кбіт/с	Байт передачі повідомлень статусу системи синхронізації
Байти, що зарезервовані для національних операторів зв'язку	Інші байти заголовку MSON, або зарезервовані для національних операторів зв'язку, або не використовуються
Поля показчиків H1, H2, H3 задають положення початку віртуального контейнера VC-4, або трьох віртуальних контейнерів VC-3 відносно поля показчиків	

Тому мультиплексор вставляє три “холостих” байти в дані віртуального контейнера, після чого продовжує заповнення VC-4 “підоспілими” за час паузи користувальницькими даними. Показчик збільшується на одиницю, що відбиває запізнення початку чергового контейнера VC-4 на три байти. Ця операція над показчиком називається позитивним вирівнюванням. У підсумку середня швидкість

користувальницьких даних, що відправляють, стає рівною швидкості їх надходження, без вставки додаткових бітів у стилі PDH. Якщо швидкість надходження даних VC-4 вище, ніж швидкість відправлення кадру STM-1, то у мультиплексорі періодично виникає потреба вставки в кадр “зайвих” байтів, для яких у поле VC-4 немає місця. Для їх розміщення використовуються три молодших байти покажчика, тобто поле НЗ (саме значення покажчика вміщається в поля Н1 і Н2). Покажчик при цьому зменшується на одиницю, тому така операція називається негативним вирівнюванням.

Типові топології. У мережах SDH застосовуються різні топології зв'язку. Найбільш часто використовуються кільця й лінійні ланцюги мультиплексорів, також знаходить все більше застосування комірчаста топологія, яка близька до повнозв'язаної.

Кільце SDH будується з мультиплексорів введення-виведення, що мають, принаймні, по два агрегатних порти (рис. 9.8, а). Користувальницькі потоки вводяться в кільце й виводяться з кільця через трибутарні порти, створюючи двопунктові з'єднання (на рисунку показані як приклад два таких з'єднання). Кільце є класичною регулярною топологією, що володіє потенційною відмовостійкістю – при однократному обриві кабелю або виході з ладу мультиплексора з'єднання збережеться, якщо його направити по кільцю в протилежному напрямку. Кільце звичайно будується на основі кабелю із двома оптичними волокнами, але іноді для підвищення надійності й пропускної здатності застосовують чотири волокна.

Ланцюг (рис. 9.8, б) – це лінійна послідовність мультиплексорів, з яких два прикінцевих відіграють роль термінальних мультиплексорів, а інші – мультиплексорів введення-виведення.

Зазвичай мережа з топологією ланцюга застосовується в тих випадках, коли вузли мають відповідне географічне розташування, наприклад, уздовж магістралі залізниці або трубопроводу. Правда, у таких випадках може застосовуватися й плоске кільце (рис. 9.8, в), що забезпечує більш високий рівень відмовостійкості за рахунок двох додаткових волокон у магістральному кабелі й по одному додатковому агрегатному порту в термінальних мультиплексорах.

Ці базові топології можуть комбінуватися при побудові складної й розгалуженої мережі SDH, створюючи ділянки з радіально-кільцевою топологією, з'єднаннями “кільце-кільце” і т.п. Найбільш загальним випадком є комірчаста топологія мережі (рис. 9.8, г), при якій мультиплексори

з'єднуються один з одним великою кількістю зв'язків за рахунок чого мережа може досягти високого ступеня продуктивності й надійності.

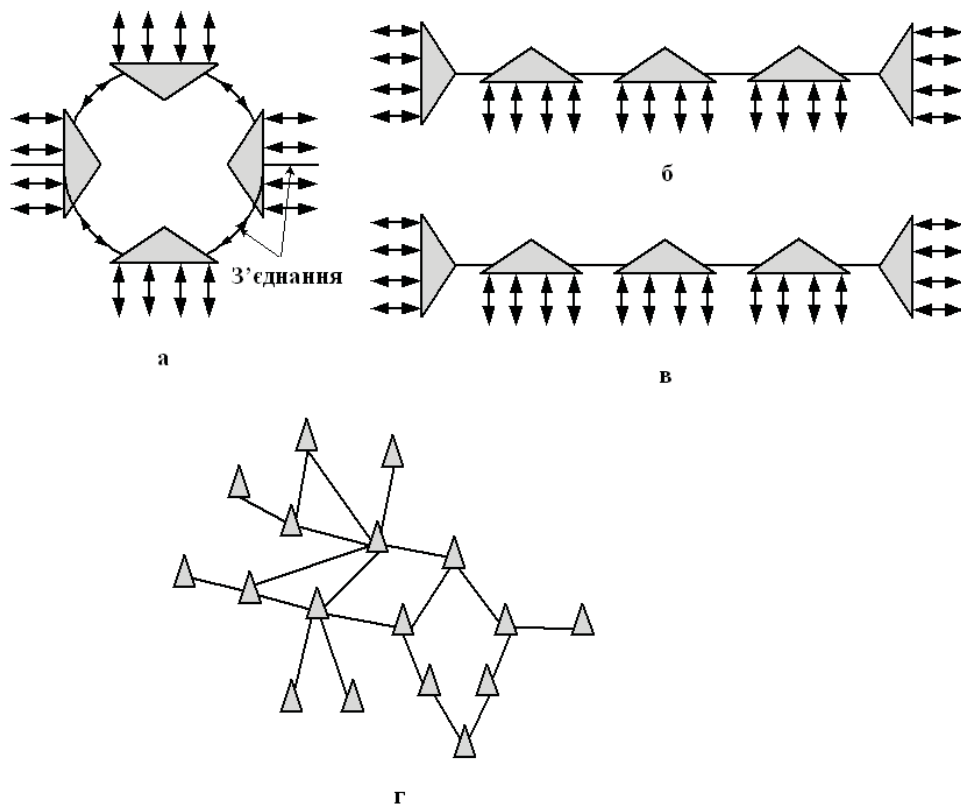


Рис. 9.8. Типові топології SDH

9.3. Глобальні мережі з комутацією каналів

Існує два типи віртуальних каналів. *Комутуючий віртуальний канал* (Switched Virtual Circuit, SVC), створення якого відбувається з ініціативи прикінцевого вузла мережі за допомогою автоматичної процедури. *Постійний віртуальний канал* (Permanent Virtual Circuit, PVC), його створення відбувається заздалегідь, причому комутатори настраюються власноруч адміністратором мережі, можливо, із залученням централізованої системи мережного адміністрування й деякого службового протоколу.

Процедура створення комутуючого віртуального каналу, подібна до процедури встановлення з'єднання в телефонних мережах. У телефонних мережах протокол, що реалізує таку процедуру, називається сигнальним протоколом, тому й протоколи встановлення віртуального з'єднання в мережах з комутацією пакетів також часто називають сигнальними. Створення комутуючого віртуального каналу вимагає наявності в комутаторах таблиць маршрутизації, аналогічних таблицям маршрутизації дейтаграмних мереж, наприклад IP-мереж. При цьому неважливо, як вони

були побудовані, автоматично, за допомогою якого-небудь протоколу маршрутизації, або вручну. Приклад такої таблиці наведений на рис. 9.9.

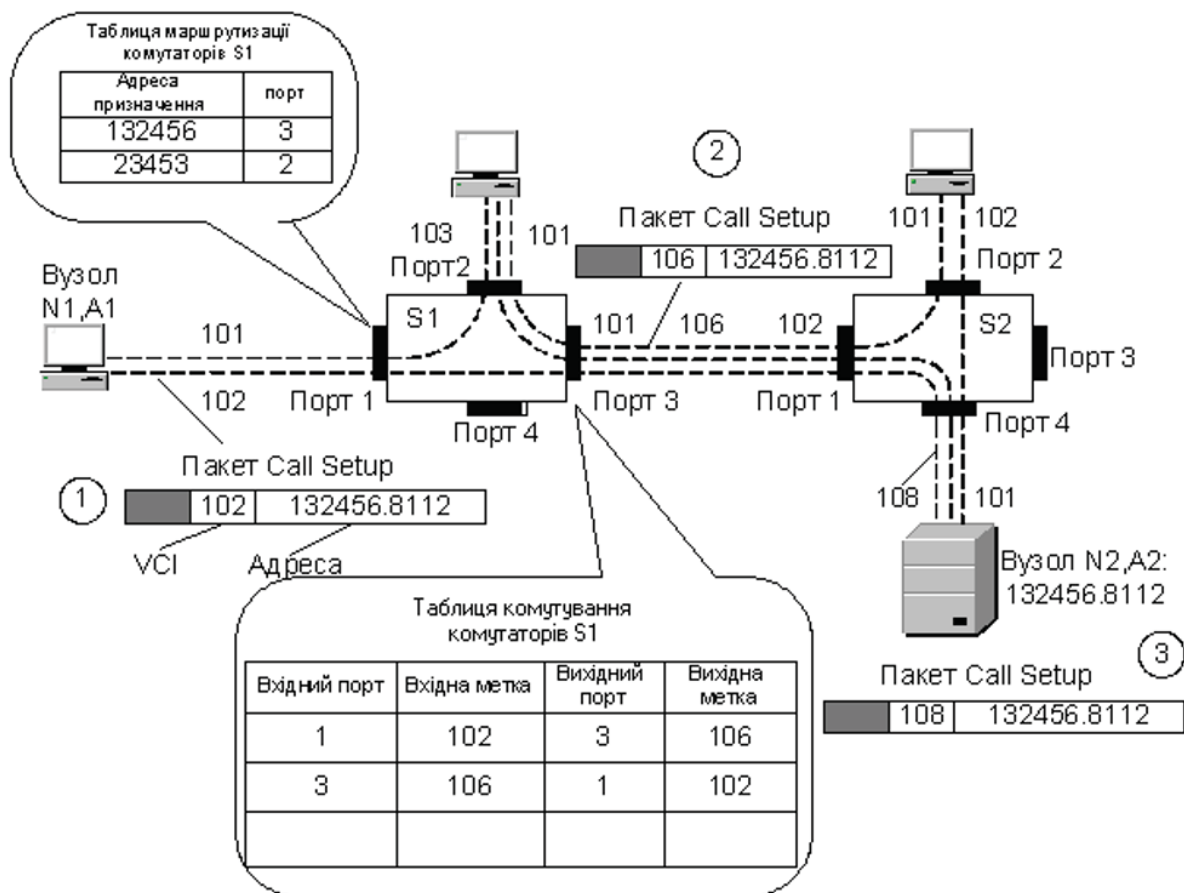


Рис. 9.9. Встановлення віртуального каналу

Рис. 9.9 ілюструє процес прокладання віртуального каналу між вузлами N1, A1 і N2, A2 через мережу, представлену тут двома комутаторами S1 і S2. На рисунку позначені три описаних нижче етапи виконання цієї процедури.

1. Встановлення віртуального каналу починається з того, що вузол ініціатор N1, A1 генерує спеціальний пакет – запит на встановлення логічного з'єднання з вузлом N2, A2. У прикладі цей запит названий Call Setup (таку ж назва він носить і в деяких конкретних сигнальних протоколах, наприклад в Q.933 для Frame Relay і Q.2931 для ATM). Спрощено можна сказати, що запит містить пари: багаторозрядну адресу вузла призначення й початкове значення ідентифікатора віртуального каналу (VCI). У прикладі на самому початку запит Call Setup має початковий вигляд: (102, 132456.8112).

При цьому 102 – початкове значення VC1, а 132456.8112 – адреса вузла призначення, старша частина якого – номер підмережі, молодша частина – номер вузла.

Привласнений віртуальному каналу номер 102 має локальне значення для порту комп'ютера, через який встановлюється з'єднання, тому що через порт уже проходить віртуальний канал з номером 101. Програмне забезпечення сигнального протоколу, що працює на прикінцевому вузлі, просто вибрало перший вільний не використовуваний у цей момент на даному порту номер з дозволеного діапазону. Такий підхід гарантує унікальну ідентифікацію віртуальних каналів у межах кожного порту.

Вузол ініціатор повинен вибрати комутатор мережі, якому доцільно передати запит на встановлення каналу. Такий вибір може відбуватися на основі таблиці маршрутизації вузла відправника, але якщо вузол з'єднаний з мережею єдиним портом, то таблиця маршрутизації вузла не потрібна. Потрапивши в буфер порту 1 комутатора S1, пакет Call Setup обробляється у відповідності зі своєю адресою призначення та значеннями таблиці маршрутизації. Запис із адресою 132456 говорить, що пакет потрібно передати на порт 3.

2. Після визначення для пакета Call Setup вихідного порту комутатор S1 генерує для нього нове значення номера віртуального каналу, а саме 106. Цей номер був обраний тому, що на ділянці мережі від порту 3 комутатора S1 до порту 1 комутатора S2 він однозначно ідентифікує встановлюваний віртуальний канал. Після зміни значення ідентифікатора віртуального каналу пакет Call Setup здобуває вид (106, 132456.8112) і передається через вихідний порт 3 комутатора S1 на вхідний порт 1 комутатора S2.

Одночасно із просуванням пакета комутатор створює таблицю комутації. Таблиця комутації буде потрібна згодом, коли віртуальний канал буде встановлений і по ньому почнуть передаватися користувальницькі дані, причому вже без адрес вузлів призначення.

Кожний запис таблиці комутації складається із чотирьох основних полів:

- номера вхідного порту;
- вхідної мітки (SVC) у пакетах, які поступають на вхідний порт;
- номера вихідного порту;
- вихідної мітки (SVC) у пакетах, що передаються через вихідний порт.

У таблиці комутації запис 1-102-3-106 означає, що всі пакети, які надійдуть на порт 1 з ідентифікатором віртуального каналу 102, будуть просуватися на порт 3, а в полі ідентифікатора віртуального каналу з'явиться нове значення – 106.

Віртуальні канали можуть бути односпрямованими й двоспрямованими. У розглянутому прикладі створюється двоспрямований канал, тому комутатор створює ще один запис у таблиці комутації – для просування пакетів у зворотному напрямку, від вузла N2, A2 до вузла N1, A1. Цей запис є дзеркальним стосовно першого запису, так що пакет, що має мітку 106 і надійшов на порт 3 комутатора S1, одержить при виході з порту 1 первісне значення мітки, а саме 102. В результаті вузол N1, A1 правильно розпізнає приналежність пакета, що прийшов по віртуальному каналу, незважаючи на постійні зміни номерів у процесі подорожі пакета по мережі.

3. Процедуру встановлення віртуального каналу продовжує комутатор S2. За адресою призначення, зазначеною в запиті, і по своїй таблиці маршрутизації (на рисунку вона не наведена) він визначає вихідний порт і передає на нього запит, оновляючи при цьому поле ідентифікатора віртуального каналу. У цьому випадку комутатор призначив пакету Call Setup номер віртуального каналу 108. В результаті запит приходить до прикінцевого вузлу у вигляді (108, 132456.8112). Прикінцевий вузол, одержавши запит, може його прийняти або відкинути. Про позитивне рішення, тобто про встановлення віртуального каналу, він повідомляє службовим пакетом Connect, що проходить по мережі у зворотному напрямку, використовуючи “дзеркальні” записи в таблиці комутації.

Після одержання підтвердження Connect прикінцеві вузли можуть почати користуватися прокладеним віртуальним каналом, посилаючи по ньому користувальницькі дані. Відправлені вузлом N1, A1 комірки просуваються на основі значення ідентифікатора віртуального каналу, що звичайно має невелику довжину, наприклад, у технології X.25 він займає всього півтора байта, у той час як довжина адреси вузла в мережі X.25 досягає 16 байт.

По суті, в мережах на основі комутуємих віртуальних каналів використовуються два режими роботи мережі.

При прокладанні каналу SVC запит на встановлення з'єднання передається по мережі в стандартному режимі маршрутизації із глобальними (для всієї мережі) адресами призначення й інформацією про повну топологію мережі. Тобто протоколи встановлення віртуальних каналів (сигнальні протоколи) працюють на мережному рівні моделі OSI. Після встановлення з'єднання мережа починає працювати на основі локальних міток і локальних таблиць комутації, що дозволяє віднести такий режим до каналного рівня моделі OSI, а комунікаційні пристрої – до класу комутаторів.

9.3.1. Стек протоколів і структура мережі ISDN

Метою створення *технології ISDN* (Integrated Services Digital Network – цифрова мережа з інтегрованим обслуговуванням) була побудова всесвітньої мережі, що повинна була прийти на зміну телефонної мережі, доступної і розповсюдженій, й надавати мільйонам своїх користувачів різноманітні послуги, як телефонні, так і з передачі даних [3; 16]. Передача телевізійних програм по ISDN не передбачалася, тому було вирішено обмежитися пропускнуою здатністю для масових користувачів в 128 Кбіт/с.

Якби ціль розроблювачів ISDN була досягнута повною мірою, то проблема доступу домашніх користувачів до Інтернету і корпоративних мереж була б повністю вирішена. Однак з багатьох причин впровадження ISDN відбувалося дуже повільно. Процес, що почався в 80-і роки, розтягся більше десяти років, так що до моменту появи в будинках користувачів деякі послуги ISDN просто морально застаріли. Так, швидкість доступу 128 Кбіт/с сьогодні вже не є достатньою для всіх користувачів. Існує, щоправда, інший інтерфейс ISDN, що забезпечує швидкість доступу до 2 Мбіт/с, але він забагато коштує для масового користувача і його звичайно використовують тільки підприємства для підключення своїх мереж. Послуги, що надаються мережею ISDN представлені на рис. 9.10.

Базовою швидкістю мережі ISDN є швидкість каналу DS-0, тобто 64 Кбіт/с. Ця швидкість орієнтується на найпростіший метод кодування голосу – PCM, хоча диференційне кодування дозволяє передавати голос з тією ж якістю на швидкості 32 або 16 Кбіт/с.

Однією з оригінальних ідей, покладених в основу ISDN, є спільне використання принципів комутації каналів і пакетів. Однак мережа з комутацією пакетів, що працює в складі ISDN, виконує тільки службові функції – за допомогою цієї мережі передаються повідомлення сигнального протоколу. Основна інформація, тобто сам голос, як і раніше передається за допомогою мережі з комутацією каналів. У такому розподілі повідомлення про виклик абонентів утворюють пульсуючий трафік, тому його ефективніше передавати по мережі з комутацією пакетів.

Користувальницький інтерфейс заснований на каналах трьох типів: В, D і Н.

Канали типу В забезпечують передачу користувальницьких даних (оцифрованого голосу, комп'ютерних даних або суміші голосу й даних) і з більш низькими швидкостями, ніж 64 Кбіт/с. Поділ даних виконується за

допомогою техніки TDM. Поділом каналу В на підканали в цьому випадку повинне займатися користувальницьке обладнання, мережа ISDN завжди комутує цілі канали типу В. Канали типу В можуть з'єднувати користувачів за допомогою техніки комутації каналів один з одним, а також утворювати так звані напівпостійні з'єднання, які еквівалентні з'єднанням виділених каналів звичайної телефонної мережі. Канал типу В може також підключати користувача до комутатора мережі Х.25.

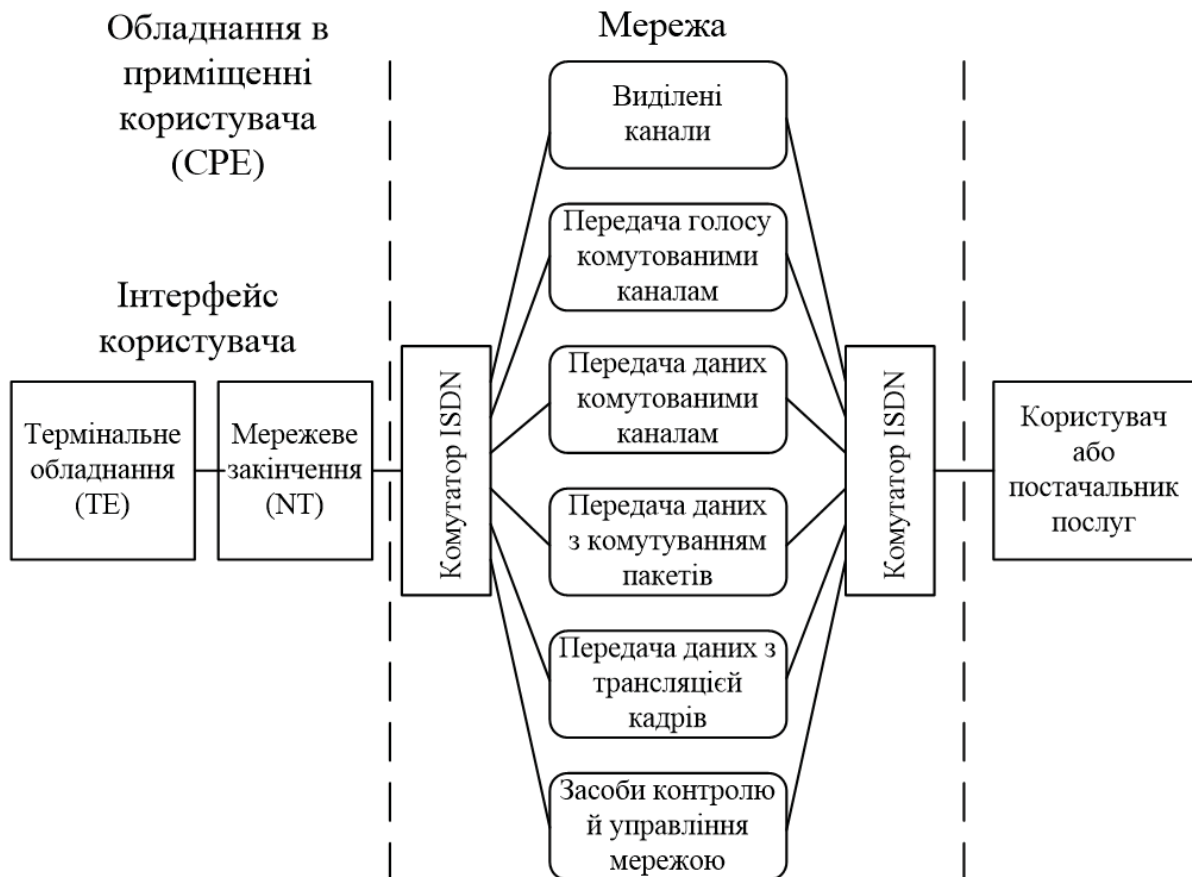


Рис. 9.10. Послуги мережі ISDN

Канал типу D є каналом доступу до службової мережі з комутацією пакетів, що передає сигнальну інформацію зі швидкістю 16 або 64 Кбіт/с. Передача адресної інформації, на основі якої здійснюється комутація каналів типу В у комутаторах мережі, є основною функцією каналу D. Іншою його функцією є підтримка послуг низькошвидкісної мережі з комутацією пакетів для користувальницьких даних. Зазвичай ця послуга виконується мережею в той час, коли канали типу D вільні від виконання основної функції.

Канали типу Н надають користувачам можливості високошвидкісної передачі даних зі швидкістю 384 Кбіт/с (Н0), 1536

Кбіт/с (Н11) або 1920 Кбіт/с (Н12). На них можуть працювати служби високошвидкісної передачі факсів, відеоінформації, якісного відтворення звуку.

Користувальницький інтерфейс ISDN являє собою набір каналів визначеного типу й з визначеними швидкостями. Мережа ISDN підтримує два види користувальницького інтерфейсу – початкових (Basic Rate Interface, BRI) і основних (Primary Rate Interface, PRI) швидкостей передачі даних.

Початковий інтерфейс ISDN надає користувачу два канали по 64 Кбіт/с для передачі даних (канали типу В) і один канал із пропускнуою здатністю 16 Кбіт/с для передачі керуючої інформації (канал типу D). Всі канали працюють у дуплексному режимі. В результаті сумарна швидкість інтерфейсу BRI для користувальницьких даних становить 144 Кбіт/с по кожному напрямку, а з урахуванням службової інформації – 192 Кбіт/с. Різні канали користувальницького інтерфейсу розділяють той самий фізичний дводротовий кабель за технологією TDM, тобто є логічними, а не фізичними каналами. Дані по інтерфейсу BRI передаються кадрами, що складаються з 48 біт. Кожний кадр містить по 2 байти кожного із двох каналів В, а також 4 біти каналу D. Передача кадра триває 250 мс, що забезпечує швидкість передачі даних 64 Кбіт/с для каналів В і 16 Кбіт/с – для каналу D. Крім бітів даних кадр містить службові біти для синхронізації кадрів та забезпечення нульового постійного складового електричного сигналу. Інтерфейс BRI може підтримувати не тільки схему 2В + D, але й В + D і просто D.

Основний інтерфейс ISDN призначений для користувачів з підвищеними вимогами до пропускнуої здатності мережі. Інтерфейс PRI підтримує або схему 30В + D, або схему 23В + D. В обох схемах канал D забезпечує швидкість 64 Кбіт/с. Перший варіант призначений для Європи, другий – для Північної Америки і Японії. Через велику популярність швидкості цифрових каналів 2,048 Мбіт/с у Європі й швидкості 1,544 Мбіт/с в інших регіонах привести стандарт на інтерфейс PRI до загального варіанта не вдалося.

Можливі варіанти інтерфейсу PRI з меншою кількістю каналів типу В, наприклад 20В + D. Канали типу В можуть поєднуватися в один логічний високошвидкісний канал із загальною швидкістю до 1920 Кбіт/с. При установці декількох інтерфейсів PRI всі вони можуть мати один канал типу D, при цьому кількість каналів В в інтерфейсі, що не має каналу D, може збільшуватися до 24 або 31.

Основний інтерфейс може бути також заснований на каналах типу Н. При цьому загальна пропускна здатність інтерфейсу не повинна перевищувати 2,048 або 1,544 Мбіт/с. Для каналів Н0 можливі інтерфейси $3Н0 + D$ для американського варіанта й $5Н0 + D$ для європейського. Для каналів Н1 можливий інтерфейс, що складається тільки з одного каналу Н11 (1,536 Мбіт/с) для американського варіанта або одного каналу Н12 (1,920 Мбіт/с) і одного каналу D для європейського варіанта. Кадри інтерфейсу PRI мають структуру кадрів DS-1 для каналів Т1 або Е1.

В мережі ISDN існує два стеки протоколів: стек каналів типу D і стек каналів типу В (рис. 9.11).

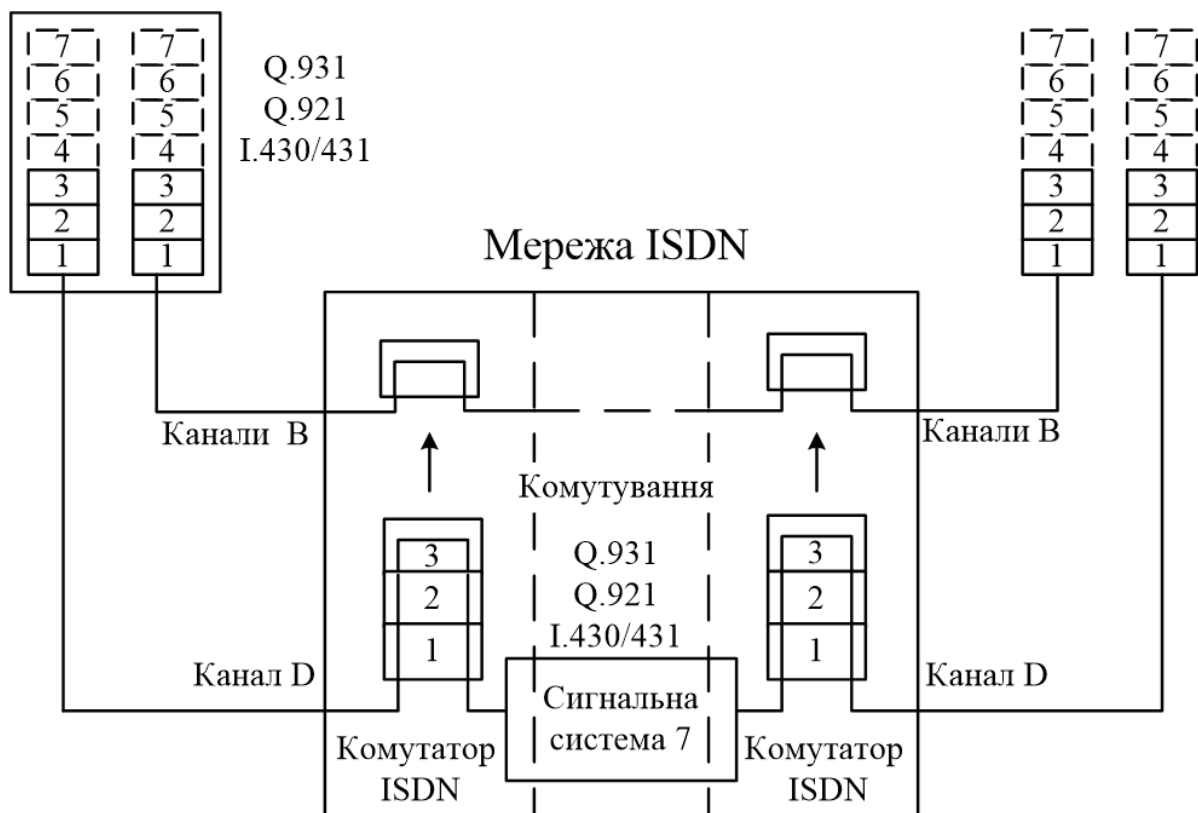


Рис. 9.11. Структура мережі ISDN

Мережа каналів типу D у середині мережі ISDN служить транспортною системою з комутацією пакетів, що застосована для передачі повідомлень сигналізації. Прообразом цієї мережі була технологія мереж Х.25. Для мережі каналів D визначені три рівні протоколів:

- фізичний протокол визначається стандартом I.430/431;
- канальний протокол LAP-D визначається стандартом Q.921;

– на мережному рівні може бути використаний протокол сигналізації Q.931, за допомогою якого виконується маршрутизація виклику абонента служби з комутацією каналів.

Канали типу В створюють мережу з комутацією каналів, що передає дані абонентів, тобто оцифрований голос. За термінами моделі OSI на каналах типу В у комутаторах мережі ISDN визначений тільки протокол фізичного рівня – протокол I.430/431. Комутація каналів типу В відбувається за вказівками, отриманими по каналу D. Коли кадри протоколу Q.931 маршрутизуються комутатором, при цьому відбувається одночасна комутація чергової частини складеного каналу від вихідного абонента до прикінцевого.

Протокол LAP-D належить до сімейства HDLC. Протокол LAP-D має всі властивості цього сімейства, але має й деякі особливості. Адреса кадру LAP-D складається з двох байтів – один байт визначає код служби, до якої пересилаються вкладені в кадр пакети, а другий потрібен для адресації одного з терміналів, якщо у користувача до абонентського кінця підключено декілька терміналів. Термінальний пристрій ISDN може підтримувати різні послуги – встановлення з'єднання за протоколом Q.931, комутації пакетів X.25, моніторингу мережі та інше. Протокол LAP-D забезпечує два режими роботи: з встановленням з'єднання й без встановлення з'єднання. Останній режим використовується, наприклад, для моніторингу мережі.

Протокол Q.931 є сигнальним протоколом ISDN для ділянки користувач-мережа, тобто протоколом типу UNI. Він переносить у своїх пакетах ISDN-адресу абонента, на підставі якої й відбувається налаштування комутаторів на підтримку складного каналу типу В.

Незважаючи на значні відмінності від аналогових телефонних мереж, мережі ISDN сьогодні використовуються в основному так само, як аналогові телефонні мережі. Тобто як мережі з комутацією каналів, але тільки більш швидкісні: інтерфейс BRI дає можливість установити дуплексний режим обміну зі швидкістю 128 Кбіт/с (логічне об'єднання двох каналів типу В), а інтерфейс PRI – 2,048 Мбіт/с. Крім того, якість цифрових каналів набагато вище, ніж аналогових. Це означає, що відсоток кадрів з помилкою буде набагато нижче, а корисна швидкість обміну даними істотно вище.

Зазвичай, інтерфейс BRI використовується в комунікаційному устаткуванні для підключення окремих комп'ютерів або невеликих локальних мереж домашніх користувачів, а інтерфейс PRI – для підключення мережі

середніх розмірів за допомогою маршрутизатора. Схема віддаленого доступу через ISDN наведена на рис. 9.12.

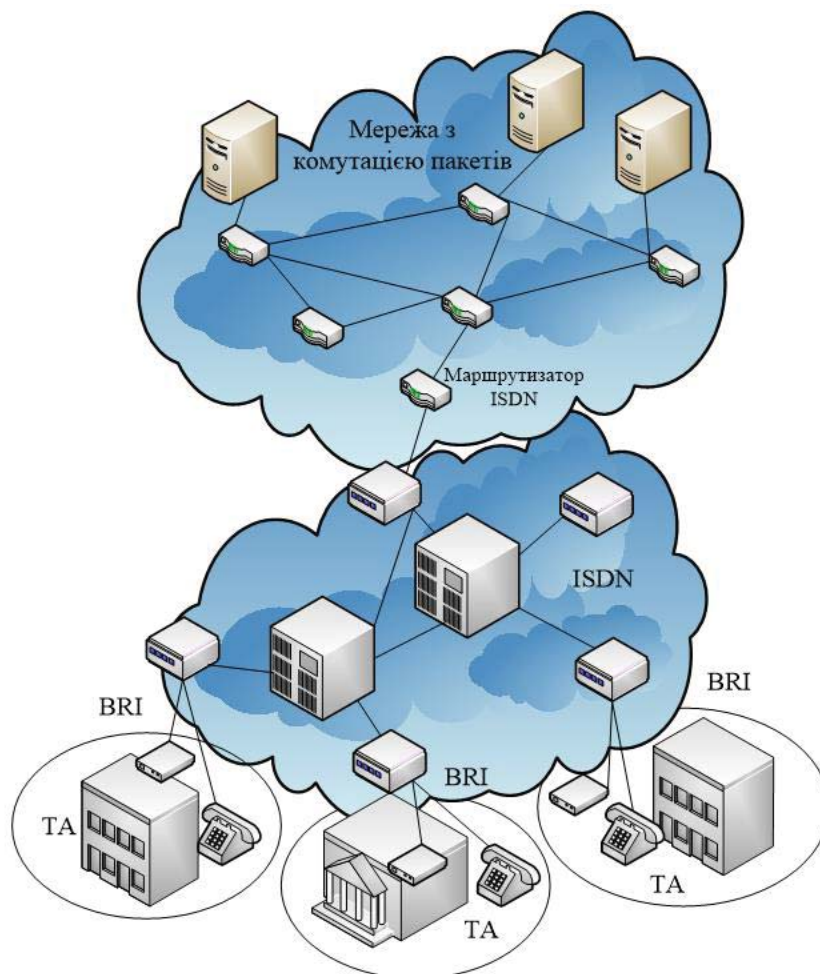


Рис. 9.12. Віддалений доступ з використанням ISDN

Підключення користувальницького обладнання до мережі ISDN здійснюється у відповідності зі схемою, розробленої ІТУ-Т (рис. 9.13). Устаткування поділяється на функціональні групи, і залежно від групи розрізняють декілька контрольних точок з'єднання різних груп обладнання між собою.

Термінальним устаткуванням 1 (ТІ1) може бути цифровий телефон або факс-апарат. Контрольна точка *S* відповідає точці підключення окремого термінального пристрою до пристрою мережного кінця (пристрій типу NT1) або концентратору користувальницьких інтерфейсів (пристрій типу NT2). ТІ1 за визначенням підтримує один з користувальницьких інтерфейсів ISDN: BRI або PRI.

Якщо термінальне обладнання ТП1 користувача підключено через інтерфейс BRI, то цифрове абонентське закінчення виконується за 2-дротовою схемою (як і звичайний кінець аналогової телефонної мережі). Для кодування даних на ділянці DSL до пункту підключення до мережі ISDN (контрольна точка U) використовується потенційний код 2B1Q. Дуплексний режим DSL створений шляхом одночасної передачі сигналів по одній витій парі в обох напрямках з відлунням-послабленням і вирахуванням свого сигналу із сумарного. Максимальна довжина абонентського закінчення для цього варіанта становить 5,5 км.

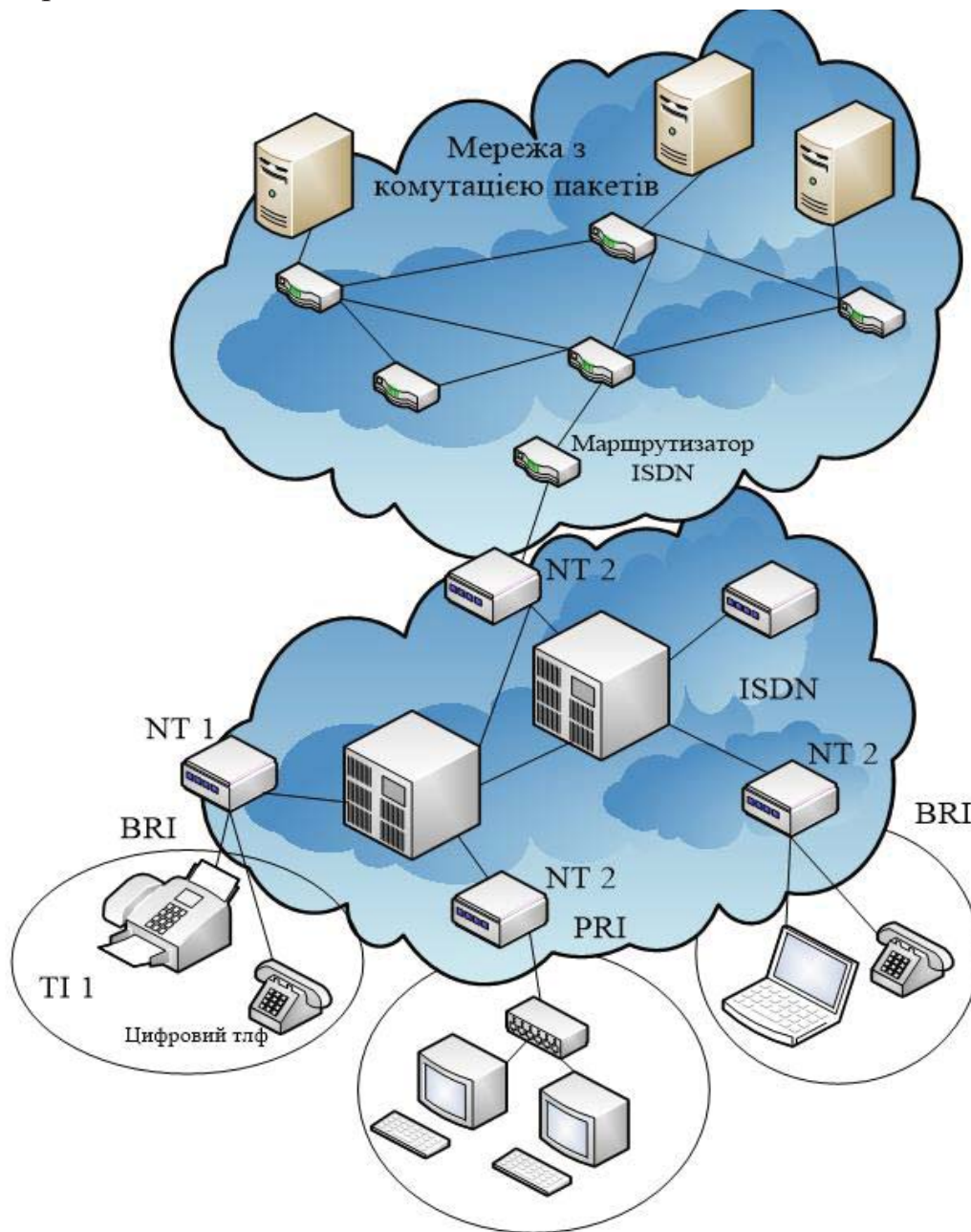


Рис. 9.13. Підключення користувацького обладнання ISDN

При використанні термінальним устаткуванням TI1 інтерфейсу PRI цифрове абонентське закінчення має являти собою канал T1 або E1, тобто 4-дротову лінію з максимальною довжиною близько 1800 м. Відповідно, на ділянці DSL до точки U використовується код HDB3 (Європа) або B8ZS (Америка).

Термінальне обладнання 2 (TI2) на відміну від TI1 не підтримує інтерфейси BRI і PRI. Таким обладнанням може бути комп'ютер, маршрутизатор з послідовними інтерфейсами, що не належать до ISDN, наприклад RS-2323, X.21 або V.35. Для підключення подібного обладнання до мережі ISDN необхідно використати термінальний адаптер. Термінальний адаптер (Terminal Adaptor, TA) узгоджує інтерфейс TI2 з інтерфейсом PRI або BRI. Для комп'ютерів термінальні адаптери випускаються у форматі мережних адаптерів. *Контрольна точка R* відповідає точці підключення термінального обладнання TI2 до адаптера TA. Тип абонентського закінчення не залежить від того, працює термінальне обладнання через TA або безпосередньо.

Пристрої мережного закінчення 2 (NT2) являють собою пристрої каналного або мережного рівня, які виконують функції концентрації користувальницьких інтерфейсів і їх мультиплексування. Наприклад, до цього типу обладнання належать: офісна АТС, комутуюча декілька інтерфейсів BRI, маршрутизатор, що працює в режимі комутації пакетів (наприклад, по каналу D), простий мультиплексор TDM, що мультиплексує декілька низькошвидкісних каналів в один канал типу В. Точка підключення обладнання типу NT2 до абонентського мережного закінчення (пристрою NT1) називається *контрольною точкою T*. Оскільки наявність даного типу обладнання не є обов'язковою (на відміну від NT1), контрольні точки S і T поєднуються й позначаються як *контрольна точка S/T*. Фізично інтерфейс у точці S/T являє собою 4-дротову лінію. Для інтерфейсу BRI, як метод кодування, обраний біполярний метод AMI, причому логічна одиниця кодується нульовим потенціалом, а логічний нуль – чергуванням потенціалів протилежної полярності. Для інтерфейсу PRI використовуються інші коди – ті ж, що й для інтерфейсів T1 і E1, тобто відповідно B8ZS і HDB3.

Пристрої мережного закінчення 1 (NT1) – це пристрої фізичного рівня, які узгоджують інтерфейс BPR або PRI із цифровим абонентським закінченням (DSL), що з'єднує користувальницьке обладнання з мережею ISDN. Фактично NT1 являє собою пристрій типу CSU, що узгоджує методи кодування, кількість використовуваних ліній і параметри електричних

сигналів. *Контрольна точка U* відповідає точці підключення пристрою NT1 до мережі.

9.4. Комп'ютерні мережі з комутацією пакетів

9.4.1. Стек протоколів і структура мережі X.25

Стандарт X.25 був розроблений комітетом CCITT в 1974 році і переглядався кілька разів. Стандарт описує не внутрішній пристрій мережі X.25, а тільки користувальницький інтерфейс із мережею, що є характерною рисою глобальних мереж. Інтерфейс цього типу називають інтерфейсом між користувачем і мережею (User-to-Network Interface, UNI). Внутрішній пристрій мережі може бути довільним, ця частина залишена на розсуд оператора мережі. На практиці комутатори глобальних мереж взаємодіють за протоколами, що аналогічні протоколам UNI. Для взаємодії між собою у мереж різних операторів зв'язку звичайно розробляється інтерфейс між ними (Network-to-Network Interface, NNI), що часто є модифікованою версією інтерфейсу UNI.

Технологія мереж X.25 має декілька істотних ознак, що відрізняють її від інших технологій.

X.25 найкраще підходить для передачі трафіку низької інтенсивності, характерної для алфавітно-цифрових терміналів 70-80 років, і в меншому ступені відповідає більш високим вимогам трафіку локальних мереж. У структурі мережі є спеціальний пристрій PAD (Packet Assembler Dissembler), що призначений для складання декількох низькошвидкісних старт-стопних потоків байтів від алфавітно-цифрових терміналів у пакети, що передаються по мережі й направляються до комп'ютерів для обробки.

Протоколи трирівневого стеку протоколів X.25 на каналному та мережному рівнях працюють із встановленням з'єднання, управляють потоками даних і виправляють помилки. Така надмірність функцій, що забезпечують надійну передачу даних, пояснюється орієнтацією технології на ненадійні лінії зв'язку з інтенсивністю у діапазоні 10^{-3} – 10^{-4} бітових помилок.

Мережний рівень розрахований на роботу тільки з одним протоколом каналного рівня й не може подібно протоколу IP поєднувати різноманітні мережі. Мережа X.25 складається з комутаторів, розташованих у різних

географічних місцях, що з'єднані високошвидкісними виділеними лініями (рис. 9.14). Виділені лінії можуть бути як цифровими, так і аналоговими

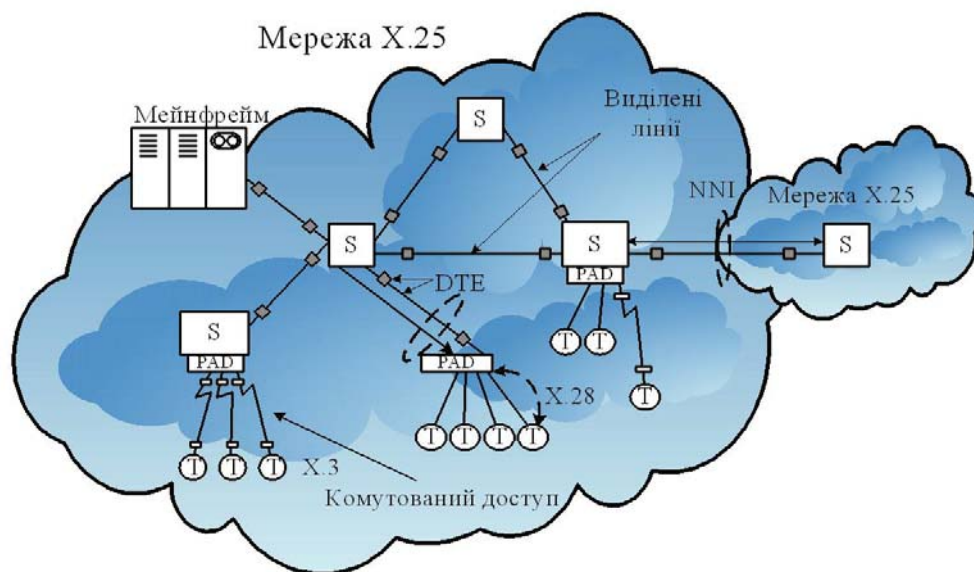


Рис. 9.14. Структура мережі X.25

Комп'ютери і локальні мережі звичайно підключаються до мережі X.25 безпосередньо через адаптер X.25 або маршрутизатор, що підтримує на своїх інтерфейсах протоколи X.25.

Якщо мережа X.25 працює автономно, то адміністратор може використати адреси будь-якої довжини (у межах формату поля адреси) і призначати адресам довільні значення. Максимальна довжина поля адреси в пакеті X.25 становить 16 байт.

Рекомендація X.121 комітету ССІТТ визначає міжнародну систему нумерації адрес для мереж передачі даних загального користування. Якщо передбачається, що мережа X.25 буде обмінюватися даними з іншими мережами X.25, то при призначенні адреси її вузлам варто дотримуватися стандарту X.121.

На *фізичному рівні* визначені синхронні інтерфейси X.21 і X.21 bis до обладнання передачі даних, або до пристроїв DSU/CSU, якщо виділена лінія є цифровою, чи до синхронного модему, якщо лінія аналогова. Протокол фізичного рівня лінії зв'язку не обговорений, і це дає можливість використовувати лінії різних стандартів.

На *канальному рівні* використовується підмножина протоколу HDLC, що забезпечує можливість автоматичної передачі у випадку помилок у лінії. На каналному рівні звичайно використовується протокол збалансованого

доступу до лінії зв'язку (Link Access Protocol – Balanced, LAP-B). Цей протокол забезпечує збалансований режим роботи, тобто обидва вузли, що беруть участь у з'єднанні, рівноправні.

На мережному рівні (у стандарті він названий не мережним, а пакетним) визначений протокол X.25/3 для обміну пакетами між прикінцевим устаткуванням і мережею передачі даних. З'єднання LAP-B забезпечують надійний зв'язок між двома сусідніми вузлами, але не дають можливості обмінюватися інформацією прикінцевим вузлам між собою. Для встановлення віртуального з'єднання між прикінцевими вузлами використовується протокол X.25/3.

9.4.2. Стек протоколів і структура мережі Frame Relay

Технологія Frame Relay була спочатку стандартизована комітетом CCITT (ITU-T) як одна з служб мереж ISDN. *Технологія ISDN* є першим широкомасштабним проектом по створенню всесвітньої універсальної мережі, що надає всі основні види послуг телефонних мереж і мереж передачі даних.

У рекомендаціях I.122, що вийшли в 1988 році, послуги з передачі даних входили до числа додаткових послуг пакетного режиму ISDN. При перегляді цих рекомендацій в 1992-93 р. з'явилися стандарти на дві нові послуги: Frame Relay і Frame Switching. Різниця між ними полягає в тому, що Frame Switching забезпечує гарантовану доставку кадрів, а Frame Relay – доставку за можливістю.

Проста та ефективна для волоконно-оптичних ліній зв'язку технологія Frame Relay відразу привернула увагу провідних телекомунікаційних компаній і організацій із стандартизації. В її становленні й стандартизації крім CCITT (ITU-T) активну участь приймали форум по ретрансляції кадрів (Frame Relay Forum, FRF) і комітет T1S1 інституту ANSI. Технологія Frame Switching так і залишилася всього лише стандартом, що ніколи не мав широкого поширення.

Стандарти Frame Relay, підготовлені ITU-T/ANSI і FRF, визначають два типи віртуальних каналів – постійні (PVC) та комутуємі (SVC). Це відповідає потребам користувачів, тому що для з'єднань, по яких трафік передається майже завжди, більше підходять постійні канали, а для з'єднань, що вимагаються тільки кілька годин на місяць, – комутуємі канали. Однак виробники обладнання Frame Relay і постачальники послуг мереж Frame

Relay почали з підтримки тільки постійних віртуальних каналів. Це значно збіднило технологію. Устаткування, яке підтримує віртуальні канали, які можна комутувати, з'явилося на ринку з великою затримкою. Саме тому технологія Frame Relay часто асоціюється тільки з постійними віртуальними каналами

Стек протоколів Frame Relay організований значно простіше, ніж стек технології X.25. Розробники технології Frame Relay, з огляду на високу якість каналів зв'язку на оптичному волокні, що з'явилися наприкінці 80-х років, порахували можливим не включати в протоколи стека функції забезпечення надійності. Незважаючи на малу ймовірність такої події, помилка все-таки відбувається, технологія Frame Relay ігнорує цю ситуацію, залишаючи роботу по відбудові загублених або кадрів з помилкою протоколам верхніх рівнів, таким як TCP.

На рис. 9.15 наведений стек протоколів технологій Frame Relay і Frame Switching у тому вигляді, у якому вони описані в рекомендаціях ITU-T. Протоколи керування виконують роботу із встановлення віртуального з'єднання, а протоколи даних передають кадри по вже встановленому віртуальному з'єднанню.

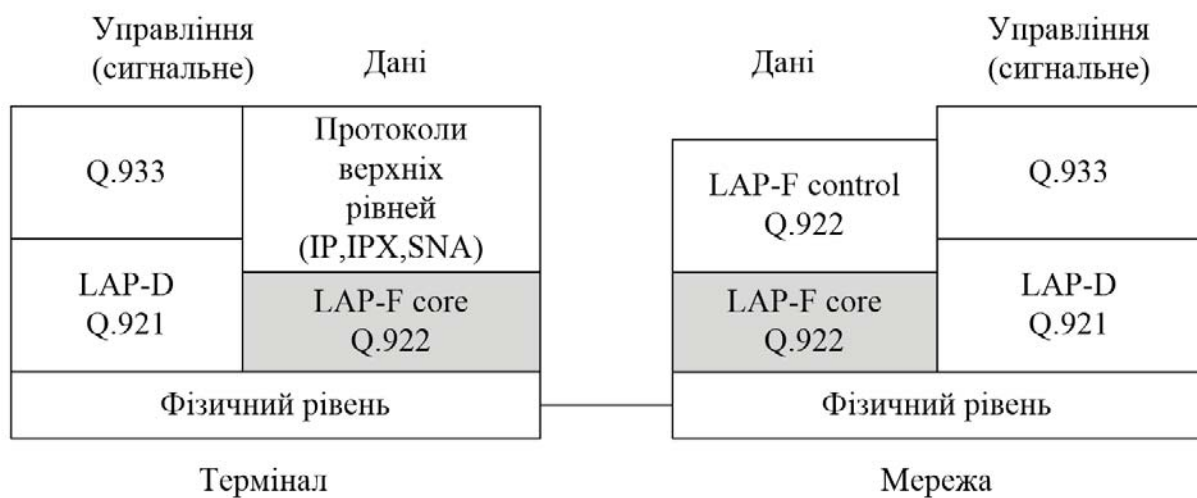


Рис. 9.15. Стек протоколів Frame Relay і Frame Switching

На каналному рівні мереж Frame Relay працює протокол LAP-F (Link Access Procedure for Frame mode bearer services), що називається у рекомендаціях ITU-T аббревіатурою Q.922. Існує дві версії цього протоколу:

1) Протокол LAP-F core забезпечує мінімум засобів, що дозволяють побудувати мережі Frame Relay. Але мережа буде надавати тільки послуги постійних віртуальних каналів;

2) Протокол LAP-F control забезпечує відновлення кадрів за алгоритмом ковзного вікна, необхідний для того, щоб мережа робила послуги Frame Switching (комутації кадрів).

Обидва протоколи (LAP-F core і LAP-F control) належать до протоколів канального рівня, забезпечуючи передачу кадрів між двома сусідніми комутаторами.

На фізичному рівні мережа Frame Relay може використати лінії зв'язку технології PDH/SDH або ISDN.

9.4.3. Стек протоколів і структура мережі АТМ

Технологія АТМ (Asynchronous Transfer Mode – асинхронний режим передачі) була розроблена як єдиний універсальний транспорт для нового покоління мереж з інтегрованим обслуговуванням, які називаються також широкосмуговими мережами ISDN (Broadband ISDN, B-ISDN) [17; 25; 26]. По суті, АТМ стала другою спробою побудови універсальної мережі після невдачі ISDN. На відміну від технології Frame Relay, що споконвічно призначалася тільки для передачі еластичного комп'ютерного трафіку, мети розробників АТМ були значно ширше.

Мережа АТМ має класичну ієрархічну структуру великої територіальної мережі – кінцеві станції з'єднуються індивідуальними лініями зв'язку з комутаторами нижнього рівня, які, у свою чергу, з'єднуються з комутаторами більш високих рівнів. Комутатори АТМ з моменту народження цієї технології підтримують як канали PVC, так і канали SVC. Для мереж АТМ визначений протокол маршрутизації PNNI (Private NNI – приватний інтерфейс NNI), за допомогою якого комутатори можуть будувати таблиці маршрутизації автоматично. У публічних мережах АТМ звичайно використовуються адреси з стандарту E.164, що робить простим взаємодію цих мереж з телефонними мережами. Адреси АТМ мають ієрархічну структуру, подібно телефонним номерам або IP-адресам, що забезпечує масштабованість мереж АТМ до будь-якого рівня, навіть загальносвітового.

У великих мережах застосовується поняття агрегованого віртуального шляху, який поєднує віртуальні канали, що мають в мережі АТМ загальний маршрут між вихідним і прикінцевим вузлами або загальною частиною маршруту між деякими двома комутаторами мережі. Ця властивість також забезпечує масштабованість мереж АТМ, тому що дозволяє істотно

скоротити кількість віртуальних з'єднань, які підтримує магістральний комутатор, тобто підвищити ефективність його роботи.

Стандарт АТМ не вводить свої специфікації на реалізацію фізичного рівня. Тут він ґрунтується на технології SDH/SONET, приймаючи її ієрархію швидкостей. Відповідно до цього початкова швидкість доступу користувача мережі – це швидкість STM-1/OC-3 155 Мбіт/с. Магістральне обладнання АТМ працює й на більш високих швидкостях STM-4 622 Мбіт/с і STM-16 2,5 Гбіт/с. Існує також обладнання АТМ, що підтримує швидкості PDH, такі як 2 або 34/45 Мбіт/с.

Кадри АТМ (називаються комірками) мають розмір 53 байта з полем даних 48 байт.

Використання в АТМ комірок такого невеликого розміру, створює відмінні умови для якісного обслуговування чутливого до затримок трафіку, але є складності. Це високий рівень навантаження на АТМ-комутатори при роботі на високих швидкостях. Обсяг роботи, що виконує комутатор або маршрутизатор будь-якої технології, прямо пропорційний кількості оброблюваних в одиницю часу пакетів, або кадрів. Очевидно, що використання комірок розмірів з полем даних 48 байт приводить до колосального росту обсягу роботи для АТМ-комутатора в порівнянні з, наприклад, комутатором Ethernet, що працює з кадрами 1500 байт. Через цю обставину АТМ-комутатори довго не могли перевершити границю швидкості інтерфейсів в 622 Мбіт/с і порівняно недавно стали підтримувати інтерфейси 2,5 Гбіт/с.

Вибір для передачі даних будь-якого типу невеликою коміркою фіксованого розміру ще не вирішує завдання сполучення різнорідного трафіку в одній мережі, а тільки створює передумови для її рішення. Для повного рішення цього завдання технологія АТМ залучає й розвиває ідеї резервування пропускної здатності і якості обслуговування, що реалізовані в технології Frame Relay.

У технології АТМ для кожного класу трафіку визначений набір кількісних параметрів, які має задати додаток. Наприклад, для трафіку класу А необхідно вказати постійну швидкість, з якої додаток буде посылати дані в мережу, а для трафіку класу В – максимально можливу швидкість, середню швидкість і максимально можливу пульсацію. Для голосового трафіку можна не тільки вказати на важливість синхронізації між передавачем і приймачем, але й кількісно задати верхні межі затримок і варіації затримок комірок.

У технології ATM прийнятий не зовсім традиційний підхід до трактування якості обслуговування QoS. Звичайна якість обслуговування трафіку характеризується параметрами пропускної здатності (RCR, SCR, MCR, MBS), параметрами затримок пакетів (CTD і CDV), а також параметрами надійності передачі пакетів (CLR). В ATM швидкісні характеристики називають параметрами трафіку й не включають їх у число параметрів якості обслуговування, хоча, по суті, вони такими є. Параметрами QoS в ATM є тільки CTD, CDV і CLR. Мережа намагається забезпечити такий рівень обслуговування, щоб підтримувалися необхідні значення й для параметрів трафіку, і для затримок комірок, і для частки загублених комірок.

Стек протоколів ATM наведений на рис. 9.16, а розподіл протоколів по прикінцевих вузлах і комутаторах ATM – на рис. 9.17.

Верхні рівні мережі

Рівні адаптації ATM (AAL 1-5)	Підрівень конвергенції (CS)	Загальна частина підрівня конвергенції
		Специфічна для сервіса частина
	Підрівень сегментації й реасемблювання (SAR)	
Рівень АТМ (маршрутизація пакетів, мультиплексування, управління потоком, обробка пріоритетів)		
Фізичний рівень	Підрівень узгодження передачі	
	Підрівень, що залежить від фізичного середовища	

Рис. 9.16. Структура стека протоколів ATM

Стек протоколів ATM відповідає нижнім рівням семирівневої моделі ISO/OSI і включає рівень адаптації ATM, власно рівень ATM і фізичний рівень. Прямої відповідності між рівнями протоколів технології ATM і рівнями моделі OSI немає.

Рівень адаптації ATM (ATM Adaptation Layer, AAL) являє собою набір протоколів AAL1 – AAL5, які перетворюють повідомлення протоколів верхніх рівнів мережі ATM в комірки ATM потрібного формату. Функції цих рівнів досить умовно відповідають функціям транспортного рівня моделі OSI, наприклад функціям протоколу TCP або UDP. Протоколи AAL при передачі

користувальницького трафіку працюють тільки в прикінцевих вузлах мережі, як і транспортні протоколи більшості технологій.

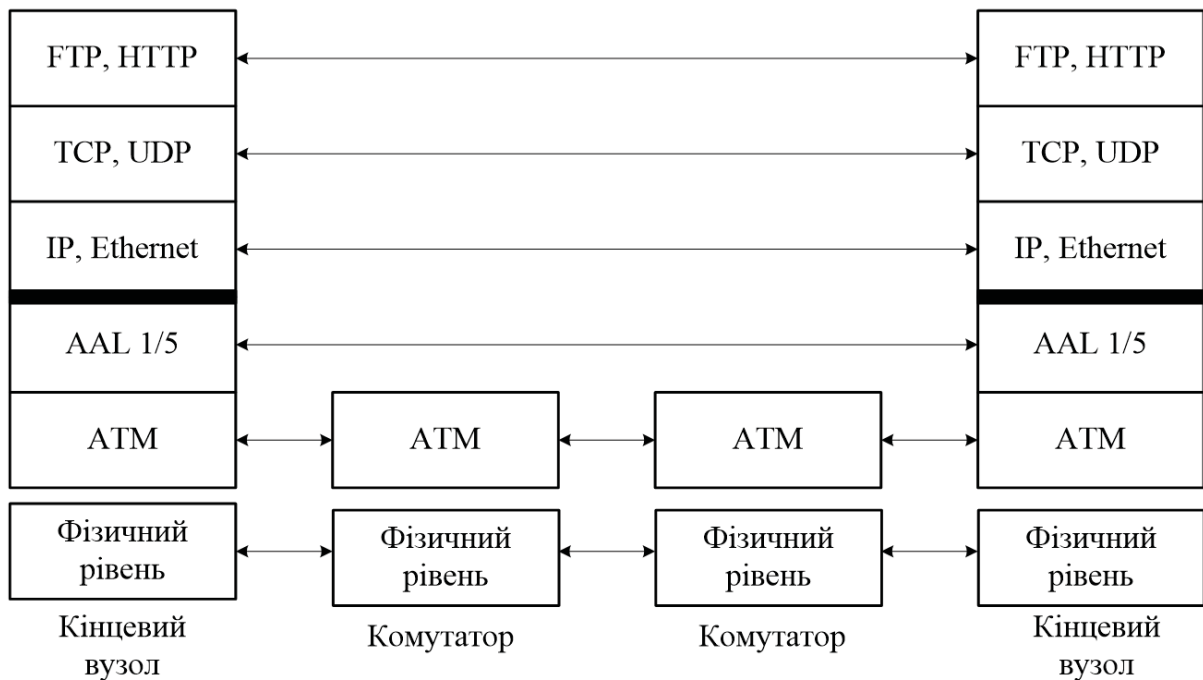


Рис. 9.17. Розподіл протоколів за вузлами і комутаторами АТМ

Кожний протокол рівня ААL обробляє користувальницький трафік визначеного класу.

Однієї із ключових ідей АТМ є гарантія якості обслуговування.

Мережа АТМ повинна однозначно й завчасно визначати свої ресурси. Мережа має підтримувати різні типи трафіку й надавати послуги різного рівня.

Керування трафіком полягає в наступному. Мережа “дивиться”, чи виконують комірки, що приходять, угоду по трафіку. Комірки, що порушують угоду (неконфорні комірки), мають встановлений біт CLP. Це означає, що вони є претендентами на скидання. Однак це не означає, що неконфорні комірки будуть обов’язково скинуті, а тільки те, що вони будуть скидатися першими при перевантаженні мережі.

Теоретично, якщо ресурси мережі визначені правильно, скидання всіх комірок із встановленим бітом CLP буде результатом підтримки рівня обслуговування в деякій точці мережі. Отже, це є критичним для досягнення мети АТМ: для гарантування якості обслуговування (або декількох типів якості обслуговування) необхідні різні типи трафіку.

Угода по трафіку ґрунтується на так званому основному алгоритмі швидкості комірок (Generic Cell Rate Algorithm – GCRA). Його називають алгоритмом “діряве відро” (continuous leaky bucket). Даний алгоритм визначає, коли потік комірок порушує або не порушує угоду по трафіку.

9.4.4. Інтерфейси DTE-DCE

Для підключення пристроїв DCE до апаратури, що формує дані для глобальної мережі, тобто до пристроїв DTE, існує декілька стандартних інтерфейсів, які є стандартами фізичного рівня. До цих стандартів відносяться стандарти серії V CCITT, а також стандарти EIA серії RS (Recommended Standards) [3; 17]. Дві лінії стандартів багато в чому дублюють одні і ті ж специфікації, але з деякими варіаціями. Дані інтерфейси дозволяють передавати дані з швидкостями від 300 біт/с до декількох мегабіт в секунду на невеликі відстані (15 – 20 м), достатні для зручного розміщення, наприклад, маршрутизатора і модему.

Інтерфейс RS-232C/V.24 є найбільш популярним низькошвидкісним інтерфейсом. Спочатку він був розроблений для передачі даних між комп’ютером і модемом з швидкістю не вище 9600 біт/с на відстань до 15 м. Пізніше практичні реалізації цього інтерфейсу стали працювати і на вищих швидкостях – до 115200 біт/с. Інтерфейс підтримує як асинхронний, так і синхронний режим роботи. Особливу популярність цей інтерфейс одержав після його реалізації в персональних комп’ютерах (його підтримують COM-порти), де він працює, як правило, тільки в асинхронному режимі і дозволяє підключити до комп’ютера не тільки комунікаційний пристрій (таке, як модем), але і багато інші периферійні пристрої – миша, графічний пристрій і т.д. Інтерфейс використовує 25-контактний з’єднувач або в спрощеному варіанті – 9-контактний з’єднувач (рис. 9.18).

Для позначення сигнальних ланцюгів використовується нумерація CCITT, яка одержала назву серія 100. Існують також двохбуквені позначення EIA, які на рисунку не показані. У інтерфейсі реалізований біполярний потенційний код $+V$, $-V$ на лініях між DTE і DCE. Зазвичай використовується досить високий рівень сигналу: 12 або 15 В, щоб надійніше розпізнавати сигнал на тлі шуму.

При асинхронній передачі даних синхронізуюча інформація міститься в самих кодах даних, тому сигнали синхронізації TxClk і RxClk відсутні. При синхронній передачі даних модем (DCE) передає на комп’ютер (DTE)

сигнали синхронізації, без яких комп'ютер не може правильно інтерпретувати потенційний код, що поступає від модему по лінії RxD. У разі коли використовується код з декількома станами (наприклад, QAM), то один тактовий сигнал відповідає декільком бітам інформації.

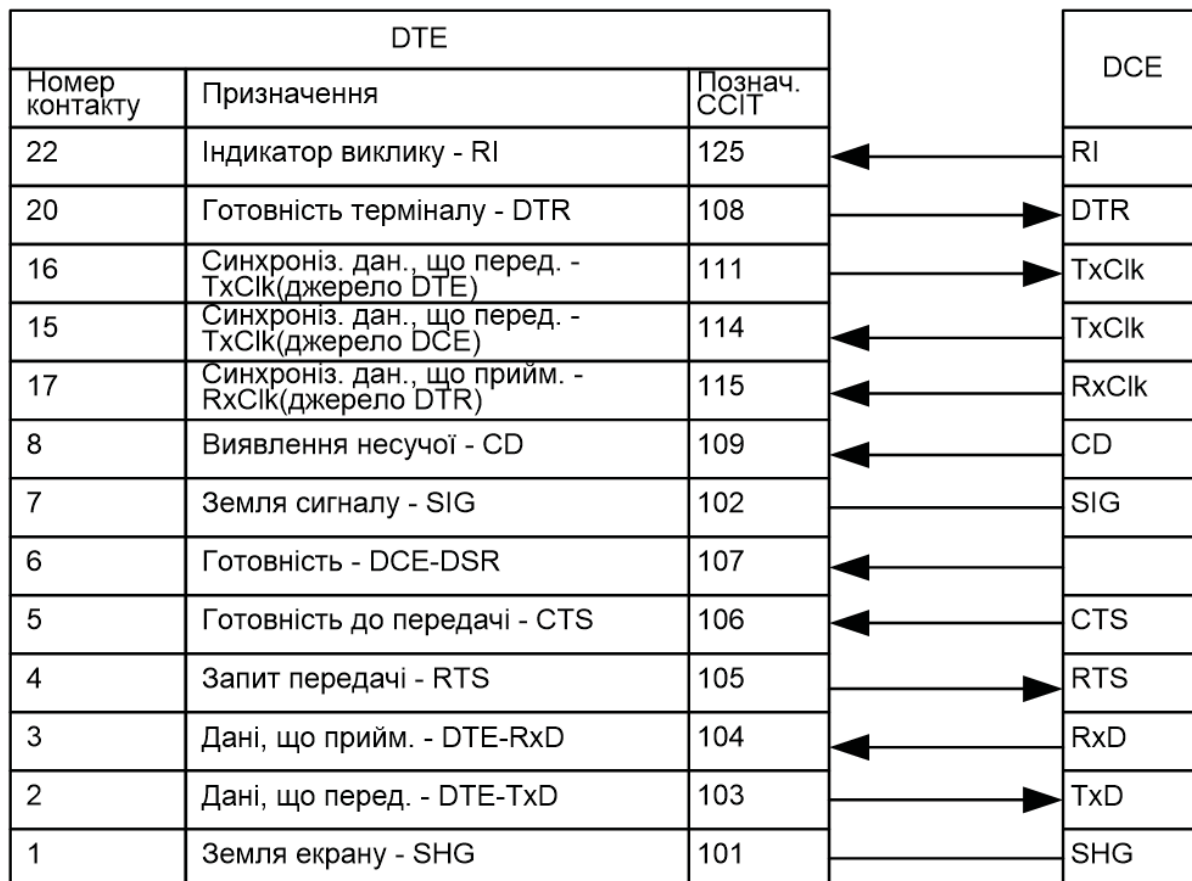


Рис. 9.18. Сигнали інтерфейсу RS-232C/ V.24

Нуль-модемний інтерфейс характерний для прямого зв'язку комп'ютерів на невеликій відстані за допомогою інтерфейсу RS-232C/V.24. В цьому випадку необхідно застосувати спеціальний нуль-модемний кабель, оскільки кожен комп'ютер чекатиме прийому даних лініями RxD, що у разі застосування модему буде коректне, але у разі прямого з'єднання комп'ютерів – ні. Крім того, нуль-модемний кабель повинен імітувати процес з'єднання і розриву через модеми, в якому використовується декілька ліній (RI, CB і т. д.). Тому для нормальної роботи двох безпосередньо сполучених комп'ютерів нуль-модемний кабель повинен виконувати наступні з'єднання:

RI-1+DSR-1- DTR-2;

DTR-1-RI-2+DSR-2;

CD-1-CTS-2+RTS-2;

CTS-1+RTS-1-CD-2;
RxD-1-TxD-2;
TxD-1-RxD-2;
SIG-1-SIG-1;
SHG-1-SHG-2.

Знак + позначає з'єднання відповідних контактів на одній стороні кабелю.

Іноді при виготовленні нуль-модемного кабелю обмежуються тільки перехресним з'єднанням ліній приймача RxD і передавача TxD, що для деякого програмного забезпечення буває досить, але в загальному випадку може привести до некоректної роботи програм, розрахованих на реальні модеми.

Інтерфейс RS-449/V.10/V.11 підтримує вищу швидкість обміну даними і велику віддаленість DCE від DTE. Цей інтерфейс має дві окремі специфікації електричних сигналів. Специфікація RS-423/V.10 (аналогічні параметри має специфікація X.26) підтримує швидкість обміну до 100000 біт/с на відстані до 10 м і швидкість до 10000 біт/с на відстані до 100 м. Специфікація RS-422/V.11(X 27 підтримує швидкість до 10 Мбіт/с на відстані до 10 м і швидкість до 1 Мбіт/с на відстані до 100 м. Як і RS-232C, інтерфейс RS-449 підтримує асинхронний і синхронний режими обміну між DTE і DCE. Для з'єднання використовується 37-контактний з'єднувач.

Інтерфейс V.35 був розроблений для підключення синхронних модемів. Він забезпечує тільки синхронний режим обміну між DTE і DCE на швидкості до 168 Кбіт/с. Для синхронізації обміну використовуються спеціальні тактуючі лінії. Максимальна відстань між DTE і DCE не перевищує 15 м, як і в інтерфейсі RS-232C.

Інтерфейс X.21 розроблений для синхронного обміну даними між DTE і DCE в мережах з комутацією пакетів X.25. Це достатньо складний інтерфейс, який підтримує процедури встановлення з'єднання в мережах з комутацією пакетів і каналів. Інтерфейс був розрахований на цифрові DCE. Для підтримки синхронних модемів була розроблена версія інтерфейсу X.21 bis, яка має декілька варіантів специфікації електричних сигналів: RS-232C, V.10, V.I 1 і V.35.

Інтерфейс струмова петля використовується для збільшення відстані між DTE і DCE. Сигналом є не потенціал, а струм величиною 20 мА, що протікає в замкнутому контурі передавача і приймача. Дуплексний обмін реалізований на двох струмових петлях. Інтерфейс працює тільки в

асинхронному режимі. Відстань між DTE і DCE може складати декілька кілометрів, а швидкість передачі – до 20 Кбіт/с.

Інтерфейс HSSI (High-Speed Serial Interface) розроблений для підключення до пристроїв DCE, що працюють на високошвидкісні канали, такі як канали ТЗ (45 Мбіт/с), SONET OC-1 (52 Мбіт/с). Інтерфейс працює в синхронному режимі і підтримує передачу даних в діапазоні швидкостей від 300 Кбіт/с до 52 Мбіт/с.

9.4.5. Введення в операції MPLS

Багатопротокольна комутація за мітками – це метод пересилання пакетів, у якому для ухвалення рішень про пересилання використовують мітки, а не IPv4-адресу призначення пакета рівня 3. MPLS зазвичай використовується в глобальних мережах (WAN) і мережах постачальників послуг для підвищення ефективності та продуктивності передачі даних. MPLS був розроблений для підтримки багатьох різних протоколів рівня 3.

MPLS знижує витрати часу на пересилання на основних маршрутизаторах, роблячи їх більш ефективними, MPLS може пересилати інші протоколи 3 рівня, окрім IPv4, MPLS також підтримує кілька сервісів, таких як одноадресна маршрутизація, багатоадресна маршрутизація, VPN, TE, QoS. Таким чином, MPLS дуже ефективний і гнучкий.

Деякі ключові характеристики та переваги MPLS:

1. *Перемикання за мітками.* MPLS використовує мітки для ідентифікації та пересилання пакетів даних мережею. Кожна мітка містить інформацію, яка допомагає маршрутизаторам ухвалювати рішення про переадресацію, забезпечуючи швидшу й ефективнішу маршрутизацію трафіку.

2. *Керування трафіком.* MPLS дає змогу мережевим адміністраторам контролювати шлях і потік трафіку в мережі. Призначаючи мітки пакетам, вони можуть застосовувати методи керування трафіком, як-от якість обслуговування (QoS) і балансування навантаження, для оптимізації продуктивності мережі та визначення пріоритетів певних типів трафіку.

3. *Віртуальні приватні мережі (VPN).* MPLS зазвичай використовується для створення безпечних і масштабованих VPN. Призначаючи мітки пакетам, MPLS може встановлювати віртуальні з'єднання між географічно розкиданими точками, забезпечуючи при цьому конфіденційність і цілісність даних. MPLS VPN широко використовуються в

корпоративних мережах для під'єднання віддалених офісів і забезпечення безпечного зв'язку.

4. *Масштабованість.* MPLS призначений для роботи у великомасштабних мережах з тисячами вузлів і високим трафіком даних. Він забезпечує масштабовану архітектуру, яка ефективно справляється зі зростаючими потребами сучасних мереж, що робить його придатним для мереж постачальників послуг і великих організацій.

5. *Ізоляція трафіку.* MPLS дає змогу ізолювати трафік, розділяючи різні типи трафіку на окремі шляхи пересилання або віртуальні канали. Ця ізоляція підвищує продуктивність, безпеку і надійність мережі, запобігаючи перевантаженню або збоєм, спричиненим одним типом трафіку, що впливає на інші.

6. *Якість обслуговування (QoS).* MPLS підтримує функції QoS, даючи змогу мережевим адміністраторам призначати пріоритети певним типам трафіку на основі зумовлених параметрів. Це гарантує, що критично важливі додатки, як-от голос або відео, отримають необхідну смугу пропускання з меншою затримкою.

Загалом, MPLS забезпечує гнучкий і ефективний механізм маршрутизації та пересилання пакетів у великих мережах. Його здатність оптимізувати потік трафіку, створювати безпечні VPN і підтримувати QoS робить його популярним для постачальників послуг і організацій, яким потрібні надійні та високопродуктивні мережеві рішення.

Інформаційна база переадресації міток (LFIB)

Інформаційна база переадресації міток (Label Forwarding Information Base, LFIB) є важливим компонентом маршрутизаторів MPLS. Вона зберігає необхідну інформацію про пересилання для вхідних пакетів на основі присвоєних їм міток. LFIB використовується для ухвалення швидких і ефективних рішень про пересилання пакетів MPLS (рис. 9.19).

Важливі аспекти інформаційної бази пересилання міток (LFIB) в MPLS:

1. *Записи міток.* Кожен запис у LFIB містить значення мітки і відповідну інформацію про пересилання. Інформація про пересилання містить такі відомості, як вихідний інтерфейс, маршрутизатор наступного переходу і будь-які конкретні операції або обробки, які необхідно застосувати до пакета.

2. *Розподіл міток.* Маршрутизатори MPLS обмінюються інформацією про відображення міток з використанням таких протоколів, як протокол поширення міток (LDP) або протокол резервування ресурсів (RSVP-TE). Ці протоколи спрощують розподіл зіставлень міток між маршрутизаторами, дозволяючи їм заповнювати свої відповідні LFIB необхідною інформацією про пересилання міток.

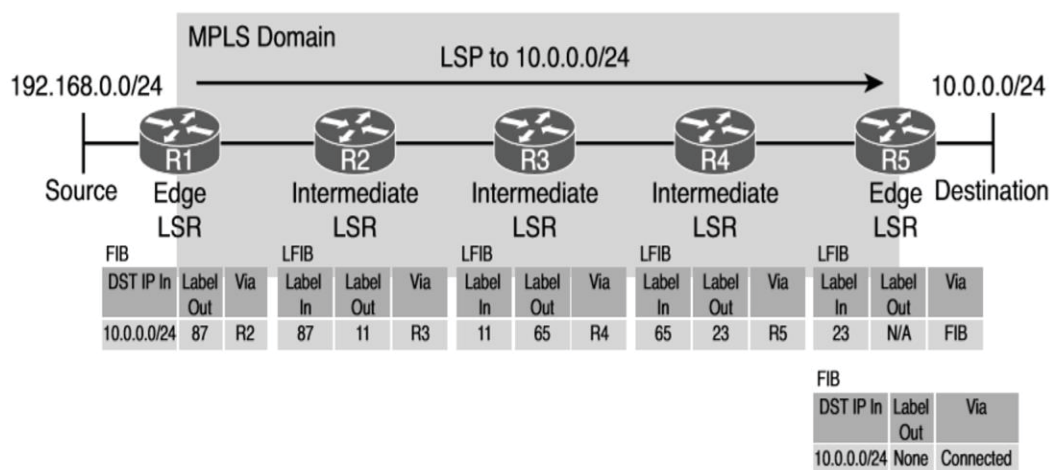


Рис. 9.19. Інформаційна база переадресації міток у MPLS

3. *Пошук мітки і пересилання.* Коли маршрутизатор MPLS отримує пакет, він перевіряє мітку в заголовку пакета. Маршрутизатор виконує пошук у своєму LFIB, щоб знайти відповідний запис мітки. На основі інформації про пересилання в записі LFIB маршрутизатор визначає відповідний вихідний інтерфейс і маршрутизатор наступного переходу для пакета. Потім пакет пересилається відповідним чином із непошкодженою міткою.

4. *Операції з мітками.* LFIB надає інструкції для операцій з мітками, як-от заміна, вштовхування і вилучення. Ці операції визначають, як маніпулюють мітками, коли пакети проходять через мережу MPLS. Обмін передбачає заміну вхідної мітки новою міткою, надсилання – додавання нової мітки в наявний стек міток, а вилучення – видалення верхньої мітки зі стека міток.

5. *Стек міток.* MPLS дає змогу накладати кілька міток у пакет. Кожна мітка в стеку міток представляє окрему операцію пересилання MPLS. LFIB допомагає маршрутизаторам ідентифікувати й обробляти мітки в стеку, даючи їм змогу виконувати відповідні операції з мітками.

6. *Масштабованість і ефективність.* LFIB призначена для ефективної роботи з великомасштабними мережами. Це дає змогу маршрутизаторам

швидко і точно визначати шлях пересилання для пакетів MPLS на основі присвоєних їм міток. Можливості швидкого пошуку LFIB сприяють загальній масштабованості та продуктивності мереж MPLS.

Інформаційна база переадресації міток (LFIB) являє собою базу даних, підтримувану маршрутизаторами MPLS для зберігання зіставлень міток і пов'язаної з ними інформації про пересилання. Вона відіграє вирішальну роль в операціях пересилання MPLS, даючи змогу маршрутизаторам ухвалювати ефективні рішення про пересилання на основі міток, присвоєних вхідним пакетам.

Протокол LDP

Протокол розподілу міток (Label Distribution Protocol, LDP) є ключовим компонентом мереж MPLS. Це сигнальний протокол, який використовують маршрутизатори для обміну інформацією про зіставлення міток, що дає їм змогу встановлювати прив'язки міток і заповнювати свою інформаційну базу пересилання міток (LFIB) необхідною інформацією про пересилання (рис. 9.20).

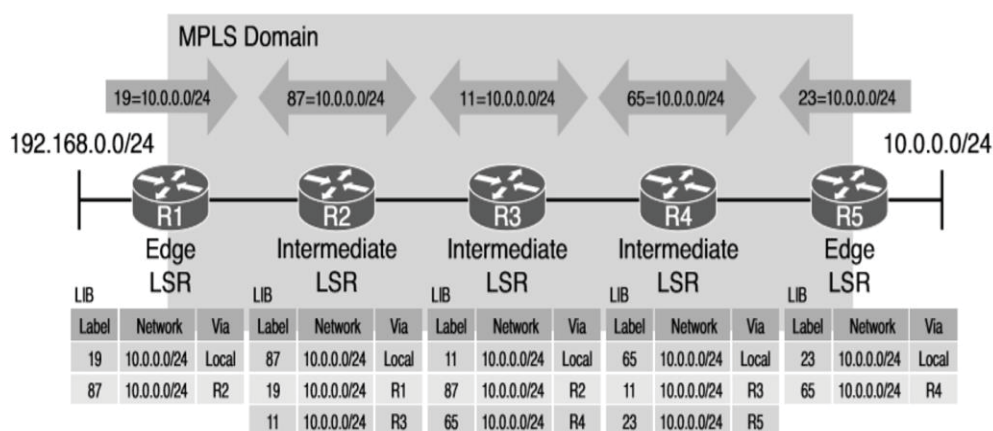


Рис. 9.20. Протокол розподілу міток у MPLS.

Основні можливості та функції протоколу розподілу міток (LDP) в MPLS:

1. *Прив'язка міток.* LDP полегшує розподіл прив'язок міток між маршрутизаторами в мережі MPLS. Прив'язка мітки – це зв'язок між мережевим префіксом або конкретним FEC (клас еквівалентності пересилання) і значенням мітки. LDP дає змогу маршрутизаторам спільно використовувати прив'язки міток, що дає їм змогу створювати узгоджений простір міток у мережі.

2. *Обмін мітками.* LDP-маршрутизатори повідомляють про свої прив'язки міток своїм сусіднім маршрутизаторам, використовуючи повідомлення LDP. Ці повідомлення містять прив'язки міток і відповідну інформацію, таку як префікс IP або FEC, пов'язані з міткою. Обмінюючись оголошеннями міток, маршрутизатори створюють єдине уявлення простору міток у мережі MPLS.

3. *Запит і поширення мітки.* Коли маршрутизатору потрібна мітка для певного FEC, він відправляє повідомлення із запитом мітки LDP на сусідній маршрутизатор. Сусідній маршрутизатор перевіряє свій LFIB на наявність запитаного FEC і відповідної прив'язки мітки. Якщо знайдено співпадаючу прив'язку мітки, маршрутизатор надсилає повідомлення зіставлення мітки LDP, що містить запитану мітку, назад запитувачу-маршрутизатору. Цей процес дає змогу маршрутизаторам розподіляти мітки для наряду пересилання.

4. *Збереження міток.* Маршрутизатори LDP зберігають прив'язки міток, отримані від своїх сусідів, для забезпечення послідовного пересилання в мережі MPLS. Зберігаючи прив'язки міток, маршрутизатори можуть швидко обробляти вхідні пакети з відповідними мітками без необхідності генерації частих повідомлень із запитами міток.

5. *Відкликання мітки.* Якщо маршрутизатору більше не потрібна певна прив'язка мітки, він відправляє своїм сусідам повідомлення про відкликання мітки LDP. Це повідомлення інформує сусідні маршрутизатори про необхідність видалити відповідну прив'язку мітки з їхнього LFIB. Відкликання мітки допомагає підтримувати синхронізоване представлення прив'язок міток по мережі.

6. *Керування та сигналізація.* LDP працює як протокол керування та сигналізації, надаючи маршрутизаторам необхідні механізми для встановлення та підтримання прив'язки міток. Це гарантує, що маршрутизатори можуть ефективно обмінюватися інформацією про зіставлення міток, підтримуючи правильне пересилання пакетів MPLS.

LDP – широко поширений протокол розподілу міток у мережах MPLS. Це дає змогу маршрутизаторам встановлювати узгоджене і синхронізоване уявлення простору міток, що дає змогу ухвалювати ефективні рішення щодо пересилання на основі зіставлень міток. Шляхом оголошення міток, запиту, утримання і відкликання LDP забезпечує належний розподіл міток і управління ними в мережі MPLS.

Як працює протокол розподілу міток у MPLS

Протокол розподілу міток (LDP) в MPLS (багатопротокольна комутація за мітками) виконує низку кроків для полегшення обміну інформацією про зіставлення міток і встановлення прив'язок міток між маршрутизаторами. Кроки роботи LDP у мережі MPLS:

1. *Виявлення сусідів.* LDP-маршрутизатори спочатку виявляють і встановлюють сусідні відносини один з одним. Зазвичай це досягається за допомогою механізму виявлення, такого як протокол Hello. Маршрутизатори LDP обмінюються повідомленнями Hello для ідентифікації сусідніх маршрутизаторів і встановлення суміжності.

2. *Оголошення міток.* Щойно відношення сусідів встановлено, маршрутизатори LDP починають повідомляти свої прив'язки міток своїм сусіднім маршрутизаторам. Прив'язки міток являють собою зв'язок між мережевими префіксами або класами еквівалентності пересилання (FEC) і значеннями міток. Кожен маршрутизатор LDP підтримує інформаційну базу міток (LFIB) для зберігання отриманих прив'язок міток.

3. *Запит мітки.* Коли маршрутизатору LDP потрібна мітка для певного FEC або префікса мережі, він відправляє повідомлення із запитом мітки LDP на сусідній маршрутизатор. Повідомлення запиту мітки містить інформацію про запитаний FEC.

4. *Зіставлення міток.* Після отримання запиту мітки сусідній LDP-маршрутизатор перевіряє свою LIB на предмет відповідності FEC і відповідної прив'язки мітки. Якщо збіг знайдено, маршрутизатор надсилає повідомлення зіставлення мітки LDP назад запитувальному маршрутизатору. Повідомлення зіставлення мітки містить запитану мітку та інформацію про пов'язаний FEC.

5. *Встановлення зв'язку міток.* Запитуючий маршрутизатор LDP отримує повідомлення зіставлення міток і встановлює зв'язування міток у своїй інформаційній базі пересилання міток (LFIB) на основі отриманого зіставлення міток. LFIB відповідає за зберігання прив'язок міток та інформації про пересилання, необхідної для ефективного пересилання пакетів.

6. *Збереження мітки.* Маршрутизатори LDP зберігають прив'язки міток, отримані від своїх сусідів, у своїх LFIB, щоб забезпечити узгоджене пересилання в мережі MPLS. Зберігаючи прив'язки міток, маршрутизатори можуть швидко обробляти вхідні пакети з відповідними мітками без необхідності частих повідомлень із запитами міток.

7. *Відкликання мітки.* Якщо маршрутизатору більше не потрібна певна прив'язка мітки, він відправляє повідомлення про відкликання мітки LDP своїм сусідам. Це повідомлення інформує сусідні маршрутизатори про необхідність видалити відповідну прив'язку мітки з їхнього LFIB. Відкликання мітки допомагає підтримувати синхронізоване представлення прив'язок міток по мережі.

8. *Керування розповсюдженням міток.* LDP містить механізми керування та сигналізації для підтримання цілісності розподілу міток. Ці механізми гарантують, що маршрутизатори можуть ефективно обмінюватися інформацією про зіставлення міток, обробляти зміни в топології мережі та реагувати на збої або додавання маршрутизаторів.

Дотримуючись цих кроків, LDP дає змогу маршрутизаторам у мережі MPLS встановлювати узгоджене уявлення простору міток і ефективно пересилати пакети на основі прив'язок міток. Зіставлення міток і обмін, підтримувані LDP, забезпечують більш швидке й ефективне пересилання трафіку MPLS.

Шлях комутації за міткою (LSP)

У MPLS шлях комутації за міткою (Label Switch Path, LSP) відноситься до шляху, яким пакет проходить через мережу MPLS на основі присвоєних йому міток. LSP встановлюється маршрутизаторами в мережі і визначає послідовність операцій з мітками, що виконуються над пакетом під час його передачі.

Етапи роботи LSP в MPLS:

1. *Призначення мітки.* Коли пакет входить у мережу MPLS, вхідний маршрутизатор присвоює йому мітку. Ця мітка представляє пункт призначення пакета або відповідну необхідну обробку пересилання. Призначена мітка зазвичай поміщається в заголовок MPLS.

2. *Пересилання міток.* Коли позначений пакет проходить через мережу MPLS, кожен маршрутизатор перевіряє вхідну мітку і виконує пошук у своїй інформаційній базі пересилання міток (LFIB). LFIB містить зіставлення міток, які пов'язують мітки з інформацією про пересилання, такою як вихідний інтерфейс і маршрутизатор наступного переходу.

3. *Операції з мітками.* На основі пошуку LFIB маршрутизатор застосовує до пакета необхідну операцію мітки. Існує три основні операції з мітками:

- *Заміна мітки*: Маршрутизатор замінює вхідну мітку новою міткою перед пересиланням пакета. Цей процес обміну дає змогу подальшим маршрутизаторам розпізнавати й обробляти пакет на основі нової мітки.

- *Вставка міток*: Маршрутизатор додає нову мітку в наявний стек міток у заголовку MPLS пакета. Зазвичай це робиться, коли необхідно виконати додаткові операції або послуги, пов'язані з MPLS.

- *Вилучення мітки*. Маршрутизатор видаляє верхню мітку зі стека міток у заголовку MPLS пакета. Ця операція зазвичай виконується, коли пакет досягає кінцевого пункту призначення або стикається з кордоном мережі MPLS. Після вилучення мітки пакет пересилається на основі базової IP-адреси або заголовка рівня 2.

4. *Пересилання на основі міток*. Після застосування необхідної операції з мітками маршрутизатор пересилає пакет на основі оновленої мітки в заголовку MPLS. Цей процес триває на кожному наступному маршрутизаторі LSP, поки пакет не досягне пункту призначення.

5. *Встановлення LSP*. Під час встановлення LSP маршрутизатори обмінюються інформацією про відображення міток за допомогою таких протоколів, як протокол поширення міток (LDP) або протокол резервування ресурсів (RSVP-TE). Це дає змогу маршрутизаторам створювати узгоджене і синхронізоване представлення простору міток у мережі MPLS.

Дотримуючись призначень міток, пересилання міток, операцій з мітками і пересилання на основі міток, мережа MPLS ефективно маршрутизує пакети за встановленим шляхом перемикання.

Маршрутизатори з комутацією за мітками (LSR)

У MPLS маршрутизатори з комутацією за мітками (Label Switch Routers, LSR) є ключовими компонентами, що відповідають за пересилання пакетів на основі присвоєних їм міток. LSR відіграють вирішальну роль у побудові та обслуговуванні маршрутів комутації за мітками (LSP) у мережі MPLS.

Характеристики та функції маршрутизаторів з комутацією міток (LSR) в MPLS:

1. *Пересилання міток*. LSR отримують пакети від сусідніх маршрутизаторів і пересилають їх на основі міток у заголовку MPLS. Кожен LSR підтримує інформаційну базу переадресації міток (LFIB), яка містить зіставлення міток і відповідну інформацію про пересилання. LFIB

використовується для визначення відповідного вихідного інтерфейсу і маршрутизатора наступного переходу для позначеного пакета.

2. *Операції з мітками.* LSR виконують операції з мітками, коли пакети проходять через мережу MPLS. Ці операції включають заміну міток, вштовхування і вилучення. Заміна мітки включає заміну вхідної мітки новою міткою перед пересиланням пакета. Простовхування мітки відноситься до додавання нової мітки до наявного стеку міток у заголовку MPLS пакета. Виштовхування мітки – це видалення верхньої мітки зі стека міток. LSR застосовують необхідні операції з мітками на основі інструкцій в LFIB.

3. *Розподіл міток.* LSR беруть участь у протоколах поширення міток, як-от протокол поширення міток (LDP) або протокол резервування ресурсів (RSVP-TE). Ці протоколи дозволяють LSR обмінюватися інформацією про відображення міток, забезпечуючи узгоджене зв'язування міток у мережі MPLS. Шляхом розподілу міток LSR заповнюють свої LFIB необхідними відображеннями міток, отриманими від сусідніх маршрутизаторів.

4. *Комутація за мітками і маршрутизація.* LSR поєднують у собі функції як комутації за мітками, так і традиційної IP-маршрутизації. Вони приймають рішення про пересилання на основі інформації про мітку, а також IP-адреси одержувача або інформації рівня 2. LSR використовують таблиці IP-маршрутизації, щоб визначити відповідну прив'язку мітки в LFIB і відповідним чином виконати переадресацію на основі мітки.

5. *Управління трафіком.* LSR підтримують можливості управління трафіком у мережах MPLS. Вони можуть застосовувати механізми якості обслуговування (QoS), методи балансування навантаження і оптимізації шляхів для забезпечення ефективної маршрутизації трафіку і використання ресурсів. LSR використовують інформацію про мітки та інформацію про пересилання в LFIB для ухвалення рішень з управління трафіком.

6. *Підтримка різних послуг в MPLS.* LSR відповідають за надання послуг на основі MPLS, таких як віртуальні приватні мережі (VPN). Вони встановлюють шляхи комутації міток (LSP) між маршрутизаторами на кордоні клієнта (CE), забезпечуючи безпечний та ізольований зв'язок між різними VPN. LSR використовують протоколи розподілу міток для обміну зіставленнями міток, характерними для VPN, і застосовують відповідні операції з мітками для пересилання трафіку всередині VPN.

Маршрутизатори з комутацією міток (LSR) є основними компонентами мереж MPLS, що виконують пересилання пакетів на основі міток. Вони підтримують LFIB, виконують операції з мітками, беруть участь у

протоколах розподілу міток, підтримують управління трафіком і забезпечують надання послуг на основі MPLS. LSR відіграють вирішальну роль у забезпеченні ефективного та надійного пересилання пакетів у мережах MPLS.

Передостанній стрибок (RHP)

Передостанній стрибок (Penultimate Hop Popping, RHP) – це метод, який використовується в мережах MPLS для оптимізації операцій з мітками і підвищення ефективності пересилання. RHP передбачає видалення передостанньої мітки з позначеного пакета на передостанньому переході до того, як він досягне кінцевого пункту призначення.

Аспекти роботи RHP в MPLS:

1. *Накладення міток.* У мережі MPLS пакетам часто призначають кілька міток, утворюючи стек міток. Мітки в стеку вказують необхідні операції пересилання на кожному переході шляхом перемикання міток (LSP).

2. *Звичайне вилучення мітки.* Зазвичай, коли помічений пакет досягає вихідного маршрутизатора (останнього маршрутизатора в LSP), остання мітка в стеку витягується, і пакет пересилається на основі базового IP-заголовка або інформації рівня 2.

3. *Передостанній перехід.* Передостанній перехід – це передостанній маршрутизатор у LSP перед тим, як пакет досягне вихідного маршрутизатора.

4. *Операція RHP.* У методі RHP маршрутизатор передостаннього переходу виконує операцію вилучення мітки, видаляючи передостанню мітку зі стека міток. Це означає, що замість того, щоб чекати, поки вихідний маршрутизатор виштовхне останню мітку, маршрутизатор передостаннього переходу бере на себе відповідальність за видалення передостанньої мітки.

5. *Рішення про пересилання.* Після вилучення передостанньої мітки маршрутизатор передостаннього переходу пересилає пакет на основі мітки, що залишилася, або базової інформації IP-заголовка.

Переваги RHP:

1. *Скорочення операцій з мітками.* Видаляючи передостанню мітку на передостанньому переході, RHP зменшує кількість операцій з мітками, що виконуються в LSP. Це допомагає підвищити ефективність пересилання і знизити навантаження на вихідний маршрутизатор.

2. *Зменшує використання ресурсів.* РНР знижує навантаження на вихідний маршрутизатор, оскільки йому більше не потрібно обробляти передостанню мітку і виконувати витяг мітки. Це може призвести до кращого використання ресурсів вихідного маршрутизатора, що дасть йому змогу ефективніше обробляти великі обсяги трафіку.

3) *Масштабованість.* За допомогою РНР мережі MPLS можуть масштабуватися більш ефективно, оскільки тягар операцій з мітками розподіляється між маршрутизаторами вздовж LSP. Це поліпшення масштабованості особливо цінне у великомасштабних мережах з високим навантаженням трафіку.

РНР є додатковою функцією MPLS і може використовуватися не у всіх розгортаннях. Його використання залежить від міркувань проектування мережі та конкретних вимог. Крім того, РНР зазвичай застосовується вибірково для певних потоків трафіку або в певних сегментах мережі, де він забезпечує найбільші переваги.

VPN рівня 3 MPLS

VPN рівня 3 MPLS (віртуальні приватні мережі) – це тип служби VPN, в якій використовується технологія MPLS для забезпечення безпечного та ізольованого зв'язку між різними сайтами або клієнтами через загальну мережеву інфраструктуру. VPN рівня 3 MPLS зазвичай використовуються підприємствами для безпечного та ефективного підключення своїх філій, віддалених сайтів або клієнтів.

VPN рівня 3 MPLS включає:

1. *Маршрутизація і пересилання VPN (VRF).* У VPN рівня 3 MPLS кожному клієнту або сайту призначається окремий екземпляр VPN-маршрутизації та пересилання (VRF). VRF – це віртуальна таблиця маршрутизації, в якій зберігаються конкретні маршрути клієнта або сайту та інформація про пересилання. Кожен VRF незалежний та ізольований від інших VRF, що забезпечує безпечний і конфіденційний зв'язок.

2. *Розподіл міток.* Мережа MPLS постачальника послуг поширює мітки на граничні маршрутизатори кожного клієнта або сайту. Ці мітки використовуються для ідентифікації та пересилання трафіку в мережі MPLS. Кожен VRF має свій унікальний набір міток.

3. *Шлях комутації за мітками (LSP).* Мітки MPLS використовуються для встановлення шляхів комутації за мітками (LSP) між граничними маршрутизаторами клієнта або сайту в мережі MPLS постачальника послуг.

LSP визначає шлях, яким пакети проходять через мережу, на основі присвоєних їм міток.

4. *Пересилання пакетів.* Коли пакет надходить на вхідний граничний маршрутизатор клієнта або сайту, маршрутизатор інкапсулює пакет за допомогою стека міток MPLS. Зовнішня етикетка відповідає VRF клієнта або об'єкта. Потім пакет пересилається на основі стека міток і таблиці маршрутизації, специфічної для VRF.

5. *Поділ VPN.* У мережі MPLS основні маршрутизатори виконують перемикання міток на основі зовнішньої мітки. Вони не знають про користувацькі маршрути або VPN. Це відокремлення базової мережі від користувацького трафіку забезпечує ізоляцію та безпеку.

6. *Вихідний маршрутизатор.* Коли помічений пакет досягає вихідного граничного маршрутизатора, зовнішня мітка, що відповідає VRF, видаляється. Потім маршрутизатор пересилає пакет на основі IP-адреси призначення в таблиці маршрутизації, специфічної для VRF. Потім пакет відправляється у відповідний пункт призначення в мережі клієнта або сайту.

Переваги VPN рівня 3 MPLS:

1. *Безпека та ізоляція.* Віртуальні приватні мережі рівня 3 MPLS забезпечують безпечний та ізольований зв'язок між різними клієнтами або сайтами. Використання VRF гарантує, що трафік кожного клієнта або сайту відокремлений від інших, що запобігає несанкціонованому доступу або перехопленню.

2. *Масштабованість.* Віртуальні приватні мережі рівня 3 MPLS мають високу масштабованість, оскільки використання міток забезпечує ефективне пересилання і маршрутизацію пакетів. Відокремлення базової мережі від призначеного для користувача трафіку дає змогу мережі обробляти великі обсяги трафіку і підтримувати зростаючу кількість віртуальних приватних мереж.

3. *Якість обслуговування (QoS).* Віртуальні приватні мережі рівня 3 MPLS підтримують механізми якості обслуговування, даючи змогу постачальникам послуг встановлювати пріоритети або диференціювати трафік залежно від конкретних вимог. Це гарантує, що критично важливі додатки або служби отримають необхідну смугу пропускання і мережеві ресурси.

4. *Просте управління.* Віртуальні приватні мережі MPLS рівня 3 забезпечують централізоване управління і контроль, спрощуючи постачальникам послуг налаштування, моніторинг і підтримку послуг VPN.

Використання VRF спрощує надання та управління користувацькою маршрутизацією і переадресацією.

У мережах MPLS Layer 3 VPN використовується технологія MPLS для забезпечення безпечного та ізольованого зв'язку між різними клієнтами або сайтами через загальну мережеву інфраструктуру. Використовуючи VRF, розподіл міток і перемикання міток, віртуальні приватні мережі MPLS рівня 3 забезпечують масштабованість, безпеку і спрощене управління для підприємств і постачальників послуг.

9.4.5. IP-телефонія

IP-телефонія – це технологія, що дозволяє використовувати Інтернет або будь-яку іншу IP-мережу для ведення телефонних розмов і передачі факсів в режимі реального часу [3; 17; 39; 40]. Особливо актуально, з економічної точки зору, використання даної технології для здійснення міжнародних і міжміських телефонних розмов або для створення розподілених телекомунікаційних телефонних мереж.

Обладнання для IP-телефонії.

Для організації телефонного зв'язку в IP-мережах використовується спеціальне обладнання – шлюзи IP-телефонії. Загальний принцип дії телефонних шлюзів IP-телефонії такий: з одного боку шлюз підключається до телефонних ліній – і може з'єднатися з будь-яким телефоном миру. З іншого боку шлюз підключений до IP-мережі – і може зв'язатися з будь-яким комп'ютером в світі. Шлюз приймає телефонний сигнал, оцифровує його, значно стискає, розбиває на пакети і відправляє через IP-мережу за призначенням з використанням протоколу IP. Для пакетів, що приходять з IP-мережі на шлюз і що направляються в телефонну лінію, операція відбувається в зворотному порядку. Обидві складові процесу зв'язку (вхід сигналу в телефонну мережу і його вихід з телефонної мережі) відбуваються практично одночасно, що дозволяє забезпечити повнодуплексну розмову. На основі цих базових операцій можна побудувати багато різних конфігурацій.

IP-телефонія спирається на дві основні операції: перетворення двонаправленої аналогової мови в цифрову форму всередині кодуючого/декодуючого пристрою (кодека) і пакування в пакети для передачі по IP-мережі. У IP-телефонії використовується особлива система передачі пакетів із звуковою інформацією, що обумовлене специфікою передачі даних по IP-мережах.

У традиційних телефонних лініях між абонентами під час розмови створюється електричний ланцюг, і цим забезпечується фіксована пропускна здатність для передачі сигналу. Тоді як IP-мережа є системою, що реалізовує принцип комутації і маршрутизації пакетів, і не надає гарантованого шляху між точками зв'язку. Вся інформація, яка передається через IP (голос, текст, зображення, і т.п.) розділяється на пакети даних, адреси точок призначення (прийому і передачі), що мають в своєму складі, і порядковий номер. Вузли IP направляють ці пакети по мережі до закінчення маршруту доставки. Після прибуття пакетів до точки призначення, для відновлення початкового об'єму впорядкованих даних використовуються порядкові номери пакетів. Для програм, де не важливий порядок і інтервал приходу пакетів, таких як e-mail, час затримок між окремими пакетами не має вирішального значення. IP-телефонія є однією з областей передачі даних, де важлива динаміка передачі сигналу, яка забезпечується сучасними методами кодування і передачі інформації. Для забезпечення стабільного телефонного зв'язку IP-мережами введені спеціальні протоколи передачі даних, наприклад, H.323 і SIP.

9.4.6. Протоколи H.323

Протокол H.323 – основоположний стандарт, прийнятий ITU-T, де описується, яким чином чутливий до затримки трафік, зокрема голос і відео, отримує пріоритет в локальних і глобальних мережах. Він складається з ряду рекомендацій (стека протоколів) з суміжних технічних питань, таких, як якість мови, стандарти кодування звукової і відеоінформації і ін. Протокол SIP (Session Initiation Protocol) прийнятий в березні 2000 року організацією IETF як стандарт RFC 2543. SIP більшою мірою відповідає ідеології TCP/IP, ніж стек протоколів H.323. Про підтримку цього протоколу заявили такі виробники як 3Com, Cisco, Ericsson, Siemens і ін. Однозначність стандарту SIP дозволяє з упевненістю говорити про сумісність IP-шлюзів різних виробників.

При передачі в режимі реального часу до 30% пакетів можуть бути загублені або отримані із запізненням (що в режимі реального часу одне і те ж). Хороший додаток IP-телефонії повинен відшкодувати брак пакетів, відновивши втрачені дані. Сам алгоритм кодування мови також робить вплив на відновлення даних.

Протокол H.323 забезпечує основу для передачі відео і аудіо інформації через IP-мережі, включаючи Internet. H.323 рекомендується ITU як набір

стандартів передачі мультимедіа інформації через локальні мережі, що не підтримують гарантованої якості сервісу QOS. Прикладами таких мереж є мережі на базі протоколів TCP/IP і IPX в середовищах Ethernet, FE, TR. Отже, протоколи H.323 є важливою частиною побудови ЛВС з підтримкою програм мультимедіа. Такі додатки включатимуть H.225, 0-RAS, Q.931-H.245, RTP/RTCP і кодеки аудіо/відео/даних (аудіо-кодеки G.711, G.723.1, G.728 і ін., відео-кодеки H.261, H.263 з компресією і декомпресією, а також кодеки даних T.120).

Мультимедіа-потoki передаються на базі протоколів RTP/ RTCP. RTP забезпечує передачу власне потоків мультимедіа, а RTCP підтримує передачу даних для управління і контролю. Сигналізація (включаючи RAS) передається за допомогою протоколу TCP. З сигналізацією мають справу наступні протоколи:

- RAS управляє реєстрацією, доступом і станом;
- Q.931 забезпечує організацію і розрив з'єднань;
- H.235 забезпечує засоби безпеки і автентифікацію;
- H.450.x – додаткові послуги.

Розташування протоколів H.323 згідно моделі OSI представлене на рис. 9.21.

Протокол RTP. Розглянемо структуру кадру RTP на рис. 9.22.

Протокол називається (real-time transport – передача в реальному масштабі часу) забезпечує транспортні функції для програм передачі даних в реальному масштабі часу (голос, відео) з використанням індивідуальних або групових адрес. RTP не резервує ресурси і не гарантує якості обслуговування QOS для сервісу в реальному масштабі часу. Протокол управління передачею RTCP підтримує використання ретрансляторів і міксерів рівня RTP.

Згідно структури кадру протоколу RTP використовуються наступні поля:

- V – версія протоколу RTP.
- P – прапор заповнення. P = 1 говорить про те, що в кінці пакету міститься один або декілька октетів вирівнювання, що не є частиною корисної інформації.
- X – біт розширення. При X = 1 після заголовка з фіксованою структурою слідує додатковий заголовок визначеного формату.

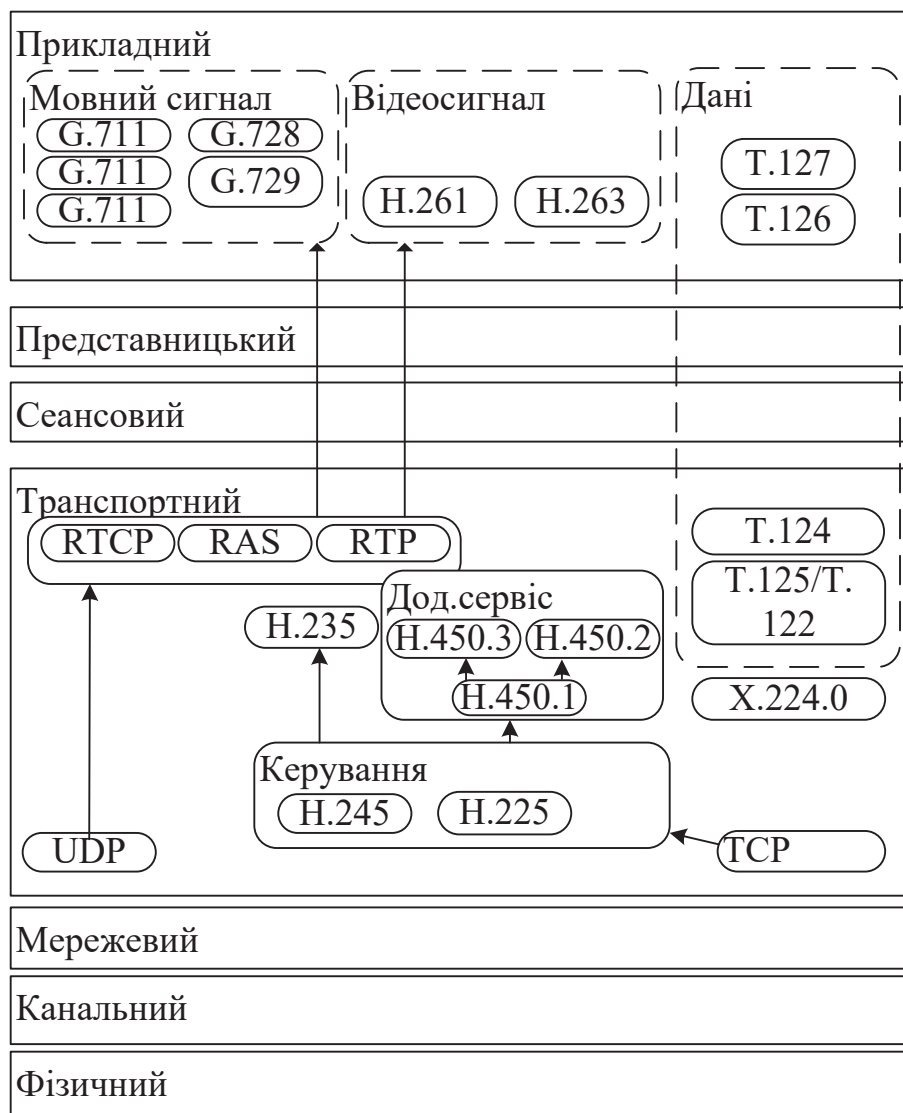


Рис. 9.21. Положення стека H.323 в еталонній моделі OSI



Рис. 9.22. Структура RTP

- *M* – маркер, інтерпретація якого визначається профілем. Маркери дозволяють відзначати важливі події (наприклад межа кадру в потоці пакетів).

- *CSRC* – лічильник *CSRC* показує кількість ідентифікаторів *CSRC*, наступних за заголовком.

- *Тип змісту* – задає формат інформаційної частини пакету *RTP* і визначає інтерпретацію пакету додатками. Використовуване за замовчанням статистичне відображення кодів типу вмісту у формати даних задається профілем. Додаткові коди типів даних можуть динамічно задаватися іншими засобами (що не відносяться до *RTP*).

- *Порядковий номер* – дане поле збільшується на одиницю для кожного наступного надсилаемого пакету *RTP*. Номер може використовуватися одержувачем для виявлення втрати пакетів і відновлення коректної послідовності пакетів.

- *Часова мітка* – відображає момент вибірки наступного октету в пакеті даних *RTP*. Значення часу вибірки повинно братися із змінної (часу), яка збільшується в часі безперервно і лінійно. Це значення використовується для синхронізації і виявлення флуктуацій часу доставки (*jitter*). Рівень дозволу годинника повинен бути достатнім для забезпечення бажаної точності синхронізації і відповідної точності визначення флуктуації часу доставки (як правило, одна зміни показань годинників на відео-кадр не достатньо).

- *SSRC* – указує джерело синхронізації (ідентифікатор вибирається випадковим чином з урахуванням того, що два джерела синхронізації в одній сесії *RTP* не повинні мати однакових ідентифікаторів *SSRC*).

- *CSRC* – список ідентифікаторів джерел інформації, що містить покажчики на джерела включеної в пакет корисної інформації.

Протокол RTCP (RFC 1889). Протокол управління *RTP* (*RTP control protocol*) ґрунтується на періодичній передачі пакетів, що управляють, всім учасникам сесії з використанням того ж механізму, який служить для передачі пакетів даних. Нижче розташований протокол рівня повинен підтримувати мультиплексування пакетів даних, що управляють (наприклад за рахунок використання різних номерів портів в *UDP*). Формат заголовка *RTCP* представлений на рис. 9.23.



Рис. 9.23. Структура кадра RTCP

V – номер версії RTP, співпадаючий для пакетів RTCP і пакетів даних RTP. В даний час використовується версія 2.+

P – прапор заповнення. P = 1 говорить про те, що в кінці пакету міститься один або декілька октетів вирівнювання, що не є частиною корисної інформації. Останній октет поля заповнення містить число октетів заповнення, які слід ігнорувати. Заповнення може бути потрібним при використанні деяких алгоритмів шифрування з фіксованим розміром блоків. У складеному пакеті RTCP заповнення може потрібно тільки для останнього з окремих пакетів, оскільки складений пакет шифрується як єдине ціле.

Лічильник прийнятих звітів – кількість блоків звіту, що містяться в пакеті. Допустиме нульове значення поля.

Тип пакету – це поле містить константу 200, яка вказує, що даний пакет відноситься до RTCP SR.

Довжина – поле довжини задає розмір пакету RTCP в 32-бітових словах мінус 1 (з урахуванням заголовка і заповнення). Зменшення реального розміру пакету робить 0 коректним значенням довжини і дозволяє уникнути зациклення при скануванні складеного пакету RTCP, а підрахунок в 32-бітових словах дозволяє уникнути перевірки кратності розміру (у октетах) числу 4.

Протокол RAS. Канал RAS (registration, admission, status – реєстрація, доступ і стан) служить для повідомлень, використовуваних в процесах виявлення шлюзів і реєстрації кінцевих точок і транспортних сигнальних транспортних каналів. Оскільки канал RAS не забезпечує гарантованої доставки, H.225.0 рекомендує використовувати для різних повідомлень таймаут і лічильники повторів. Кінцева точка або шлюз, яким не вдається відповісти на запит в течії заданого часу (таймаут), можуть використовувати

повідомлення RIP (request in progress – запит обробляється) для індикації того, що запит до цих пір не оброблений. Кінцева точка або шлюз, одержуючи RIP, обнуляють таймер і лічильник повторів.

Повідомлення RIP використовують синтаксис ASN.1.

Протокол H.225 представляє собою стандарт вузькосмугових відеотелефонних послуг, визначених в рекомендаціях H.200/AV.120. Стандарт має справу з ситуаціями, коли маршрут передачі включає, принаймні, одну мережу передачі пакетів, яка налаштована на надання якості обслуговування QOS, що не гарантується (такі мережі також не підтримують механізмів захисту і відновлення понад заданих рекомендаціями H.320 для терміналів). H.225.0 описує організацію потоків голосу, відео, даних і інформації, що управляє, в мережах передачі пакетів для забезпечення діалогового сервісу за допомогою обладнання H.323.

Структура пакетів H.225 відповідного стандарту Q.931 і наведена на рис. 9.24.

Дискримінатор протоколу – використовується для того, щоб відрізнити повідомлення, керівників викликами користувач-мережа, від інших повідомлень.

Розмір посилання – довжина поля call reference value (посилання на виклик).

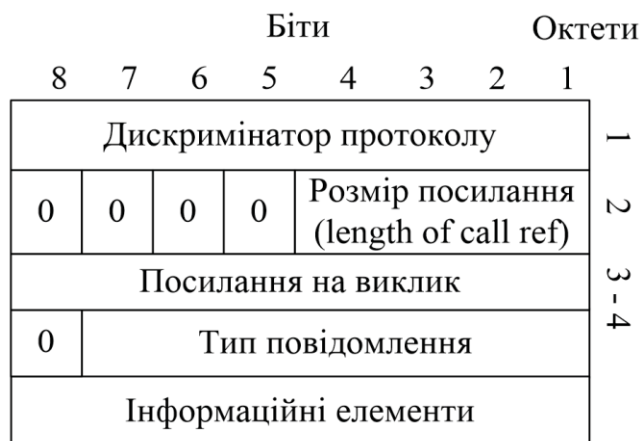


Рис. 9.24. Структура кадра H.225

Посилання на виклик – ідентифікує виклик або запит на реєстрацію/відключення пристрою на локальному інтерфейсі користувач – мережа, до якого конкретне повідомлення застосовне. Довжина посилки може складати один або два октети.

Тип повідомлення – поле типу визначає функцію переданого повідомлення. Використовуються наступні типи повідомлень:

000	xxxxxx	Повідомлення при організації з'єднань
	00001	ALERTING (попередження)
	00010	CALL PROCEEDING (обробка виклику)
	00111	CONNECT (з'єднання)
	01111	CONNECT KNOWLEDGE (підтвердження з'єднання)
	00011	PROGRESS (робота)
	00101	SETUP (встановлення)
	01101	SETUP ACKNOWLEDGE (підтвердження встановлення)
001	xxxxxx	Повідомлення при передачі інформації
	00110	RESUME (поновити)
	01110	RESUME ACKNOWLEDGE (підтвердження поновлення)
	00010	RESUME REJECT (відмова від поновлення)
	00101	SUSPEND (тимчасова зупинка)
	01101	SUSPEND ACKNOWLEDGE (підтвердження тимчасова зупинка)
	00001	SUSPEND REJECT (відмова від тимчасової зупинки)
	00000	USER INFORMATION (користувальницька інформація)
010	xxxxxx	Повідомлення при розриві з'єднань
	00101	DISCONNECT (відключення)
	01101	RELEASE (розрив з'єднання)
	11010	RELEASE COMPLETE (розрив з'єднання завершений)
	00110	RESTART (рестарт)
	01110	RESTART ACKNOWLEDGE (підтвердження рестарту)
011	xxxxxx	Інші повідомлення
	00000	SEGMENT (сегмент)
	11001	CONGESTION CONTROL (контроль перевантаження)
	11011	INFORMATION (інформація)
	01110	NOTIFY (повідомлення)
	11101	STATUS (стан)
	10101	STATUS ENQUIRY (запит стану)

Протокол визначає дві категорії інформаційних елементів – розміром в один октет і змінної довжини. Приклад формату інформаційних елементів наведений на рис. 9.25.

Формат інформаційного елементу із одного октета (тип 1)

Біти								Октет
8	7	6	5	4	3	2	1	
1	Ідентифікатор EI			Зміст IE				1

Формат інформаційного елементу із одного октета (тип 2)

Біти								Октет
8	7	6	5	4	3	2	1	
1	Ідентифікатор IE							1

Формат інформаційного елементу змінної довжини

Біти							Октет
8	7	6	5	4	3	2	1
1	Ідентифікатор ІЕ						1
Довжина змісту ІЕ						2	
Зміст ІЕ						3–n	

Рис. 9.25. Формати інформаційних елементів

Протокол H.245 визначає лінію передачі для нетелефонних сигналів. Протокол включає характеристики передачі прийому, а також переважний режим для приймальної сторони, сигналізацію логічного каналу, контроль і індикацію. Для забезпечення надійної доставки даних, аудіо і відеосигналів визначені процедури підтвердження на рівні сигналізації.

Повідомлення H.245 відповідають синтаксису ASN.1

Повідомлення типа Multimedia Control System Massage бути визначені як запит, відповідь, команда або індикація. Використовується також перераховані нижче набори додаткових повідомлень:

- Master Slave Fetermination (визначення ведучого та відомого);
- Terminal Capability (можливості терміналу);
- Logical Channel Signaling (сигналізація логічного каналу);
- Multiplex Table Signaling (сигналізація таблиці мультиплексування);

- Request Multiplex Table Signaling (запит сигналізації таблиці мультиплексування);
- Request Made (режим запиту);
- Round Trip Delay (затримка проходження сигналу в обох напрямках);
- Maintenance Loop (цикл обслуговування);
- Communication Mode (комунікаційний режим);
- Conference Request and Response (запит та відгук для конференції);
- Terminal ID (ідентифікатор терміналу);
- Comands and Indications (команди і ідентифікатори).

Протокол H.261.

Протокол H.261 описує відео-потоки для передачі за допомогою транспортного протоколу в реальному масштабі часу (RTP) (рис. 9.26). На нижчому рівні можуть використовуватися будь-які протоколи, здатні підтримувати трафік RTP.

Біти								Октет
0	1	2	3	4	5	6	7	
SBIT			EBIT			I	V	1
GOBN				MBAP				2
MBAP	QUANT					HMVD		3
HMVD			VMVD					4

Рис. 9.26. Структура заголовка H.261

SBIT – стартовий біт. Кількість старших бітів, які повинні ігноруватися в першому октеті даних.

EBIT – завершуючий біт. Кількість молодших бітів, які повинні бути проігноровані в останньому октеті даних.

I – прапор кодування даних INTRA-кадру. Якщо даний біт має значення 1, потік містить тільки блоки, що кодуються як INTRA-кадри. Нульове значення прапора говорить, що даний потік може містити або не містити блоки, що кодуються як INTRA-кадр. Значення цього біта не може змінюватися в перебігу всієї RTP-сесії.

GOBN – номер GOB, задаючий початок пакету. Значення цього поля рівне 0, якщо пакет починається із заголовка GOB.

MBAP – (Macroblock Address Predictor – прогноз адреси макроблоку) кодує прогноз адреси макроблоку (т.ч. останні значення MBA, що міститься

в попередньому пакеті). Значення поля знаходиться в діапазоні 0-32 (для прогнозу допустимих значень MBA-1-33), але оскільки бітовий потік не може бути фрагментований між заголовком GOB і MB-1, провісник на початку пакету не може бути рівний 0. Таким чином, залишається один діапазон 1 – 32, який зміщується на –1 для того, щоб було достатньо 5-бітового поля. Якщо пакет починається із заголовка GOB, поле MBAP = 0.

QUANT – поле QUANT показує значення MQUANT або GQUANT до початку пакету. Якщо пакет починається із заголовка GOB, для поля QUANT встановлюється нульове значення.

HMVD – поле HMVD (Horizontal Motion Vector Data – вектор горизонтального переміщення) є посиланням на горизонтальний вектор переміщення даних (Motion Vector Data – MVD). HMVD = 0, якщо прапор V = 0, пакет починається із заголовка GOB або для останнього MB, поміщеного в попередній пакет, значення MTYPE не рівне Mc. Значення HMVD повинне знаходитись в діапазоні –15; +15.

VMVD – поле VMVD (Vertical Motion Vector Data – вектор вертикального переміщення) є посиланням на вертикальний вектор переміщення даних (Motion Vector Data – MVD). VMVD = 0, якщо прапор V = 0, пакет починається із заголовка GOB або для останнього MB, поміщеного в попередній пакет, значення MTYPE не рівне Mc. Значення VMVD повинне знаходитись в діапазоні –15; +15.

Протокол H.263 визначає формат інкапсуляції бітового потоку H.263 в пакети RTP. Для заголовка потоку H.263 визначено три режими. Пакет RTP може використовувати один з трьох режимів відео-потoku H.263 залежно від бажаного розміру мережевого пакету і опцій кодування H.263. найкоротший заголовок H.263 (режим А) підтримує фрагментацію GOB. Довгі заголовки H.263 (режими В і З) підтримують розбиття потоку на макроблоки (MB).

Для кожного пакету RTP після заголовка RTP фіксованої довжини слідує заголовок вмісту H.263, а за ним – стислий бітовий потік стандарту H.263. Розмір заголовка вмісту H.263 залежить від використовуваного режиму. Схема відео-пакету RTP H.263 наведена на рис. 9.27.

4 байта
Заголовок RTP
Заголовок потоку H.263
Бітовий потік H.263

Рис. 9.27. Відео-пакет RTP H.263

У режимі А заголовок Н.263 містить 4 байти. Даний режим підтримує фрагментацію RTP. У режимі У використовується 8-байтовий заголовок Н.263 і кожен пакет починається на межі МВ без опцій РВ. 12-байтовий заголовок Н.263 визначає режим З, що підтримує фрагментацію на межах МВ для кадрів з опцією РВ.

Режим кожного заголовка потоку Н.263 указується значеннями полів F і Р. Пакети різних режимів можуть перемішуватися. Формат заголовка для режиму А наведений на рис. 9.28.

Біти								Октет
1	2	3	4	5	6	7	8	
F	P	SBIT			EBIT			1
SRC			I	U	S	A	R	2
R(продовження)			DBQ		TRB			3
TR								4

Рис. 9.28. Структура заголовку Н.263 для режиму А

На рис. 9.28. зображена структура заголовку Н.263 для режиму А, на якому скорочення мають наступне значення:

F – прапор, що показує режим заголовка потоку Н.263.

P – прапор необов’язкового режиму РВ, визначеного в стандарті Н.263:

0 – звичайний кадр типу I або P, 1 – кадр РВ

Якщо $F = 1$, поле *P* показує режим:

Звичайний кадр типу I або P.(0 – режим В,1 – режим З).

SBIT – стартовий біт. Кількість старших бітів, яких повинні ігноруватися в першому октеті даних.

EBIT – завершуючий біт. Кількість молодших бітів, які повинні бути проігноровані в останньому октеті даних.

SRC – вихідний формат (біти 6, 7 і 8 поля TYPE, визначуваний Н.263):

0 – Intra-кодування (внутрішнє).

1 – Inter-кодування (внутрішнє).

U – поле *U* має значення 1, якщо в поточному заголовку зображення була встановлена (1) опція необмеженого вектора переміщення (Unrestricted Motion Vector), що задається бітом 11 в полі PTYPE відповідно до визначення Н.263.

S – поле S має значення 1, якщо для поточного заголовка зображення була встановлена (1) опція синтаксичного арифметичного кодування (Syntax-base Arithmetic coding), що задається бітом 11 в полі PTYPE відповідно до визначення H.263.

Протокол H.235 забезпечує розширення рекомендацій серії H.3xx в частині додавання послуг забезпечення безпеки, такі як автентифікація і конфіденційність (authentication and privacy). H.235 повинен працювати з іншими протоколами серії H, які використовують H.245 як протокол управління. Всі повідомлення H.235 шифруються також, як в ASN.1.

Контрольні запитання

1. Що таке алгоритм маршрутизації?
2. З якою швидкістю працюють канали T-3 та T-4?
3. Які недоліки технології PDH?
4. Чим відрізняються віртуальний контейнер від трибу тарного блока або адміністративного блока?
5. Скільки строк у структурі кадру STM-1?
6. Які топології використовують в технології SDH?
7. З якою метою встановлюють віртуальні канали?
8. Яка швидкість каналів: типу В; типу D; типу Н?
9. Функції інтерфейсу BRI?
10. Які функції виконує контрольна точка R?
11. Призначення пристроїв PAD у технології X.25?
12. Функції протоколу LAP-B?
13. Максимальний розмір поля даних Frame Relay?
14. Що означає агрегований віртуальний шлях у технології АТМ?
14. Призначення поля пріоритету втрати пакету комірки АТМ?
15. З якою метою використовують нуль-модемний інтерфейс?
16. Призначення шлюзів у ІР-телефонії?
17. Призначення протоколу RTP?
18. Функції протоколу H.263?

РОЗДІЛ 10. БЕЗДРОТОВІ КОМП'ЮТЕРНІ МЕРЕЖІ

10.1. Переваги бездротового зв'язку

Бездротова локальна мережа (WLAN, Wireless LAN) – це тип бездротової мережі, яка зазвичай використовується в будинках, офісах і кампусах. Мережі повинні підтримувати людей, які знаходяться в русі. Люди під'єднуються за допомогою комп'ютерів, ноутбуків, планшетів і смартфонів. Існує безліч різноманітних мережних інфраструктур, що забезпечують доступ до мережі, наприклад, дротові локальні мережі, мережі провайдерів послуг і мережі стільникового зв'язку. Але саме WLAN робить мобільність можливою в домашніх і корпоративних середовищах.

Бездротовий зв'язок має багато переваг:

- *Мобільність:* Бездротовий зв'язок дозволяє зберігати з'єднання без фізичного обмеження кабелями, що дозволяє переміщатися і використовувати пристрої будь-де в межах зони покриття.
- *Зручність:* Відсутність потреби в кабелях полегшує налаштування та підключення пристроїв. Це також уникне плутання кабелів та створить більш організований робочий простір.
- *Ефективність:* Бездротовий зв'язок дозволяє зменшити втрати сигналу, забезпечуючи більшу стабільність і швидкість передачі даних.
- *Масштабованість:* Легко додавати нові пристрої до бездротової мережі без необхідності прокладання нових кабелів.
- *Можливість зовнішнього доступу:* Бездротовий зв'язок може бути доступним із зовнішнього середовища, такого як Wi-Fi точки доступу у кафе, готелях або громадських місцях.
- *Зручність в щоденному житті:* Бездротовий зв'язок є загальною частиною повсякденного життя, від смартфонів і планшетів до бездротових клавіатур і мишей.
- *Економія часу та ресурсів:* Відсутність необхідності у кабелях і додаткових ресурсах для їх установки і обслуговування дозволяє економити час і гроші.
- *Можливість використання в складних умовах:* Бездротовий зв'язок може бути корисним у важкодоступних місцях або під час ведення діяльності у незвичних умовах, де використання кабелів є незручним або неможливим.

10.2. Класифікація бездротових мереж

Бездротові мережі можна класифікувати за різними критеріями, такими як покриття, топологія, застосування та інші.

- **За покриттям:**

- *WPAN (Personal Area Network)*: Особиста мережа, яка покриває невелику область і призначена для особистих пристроїв, таких як Bluetooth-гарнітури.

- *WLAN (Local Area Network)*: Локальна мережа, призначена для покриття невеликої території, такої як офіс чи дом.

- *WMAN (Metropolitan Area Network)*: Мережа, яка охоплює більше місцевості, ніж LAN, але менше, ніж WAN, і використовується, наприклад, для підключення міст в одному регіоні.

- *WWAN (Wide Area Network)*: Мережа, яка покриває великі території і зазвичай використовується для підключення географічно розташованих мереж або офісів.

- **За топологією:**

- *Зірка (Star Topology)*: Всі пристрої підключені до центральної точки доступу.

- *Дерево (Tree Topology)*: Мережа має ієрархічну структуру з головною точкою доступу і підточками.

- *Змішана (Mesh Topology)*: Кожен пристрій підключений до кожного іншого пристрою у мережі.

- *Решітка (Mesh Topology)*: Кожен пристрій підключений до кількох сусідів, створюючи мережу у вигляді решітки.

- **За типом передачі даних:**

- *Аналогова бездротова мережа*: Використовує аналогові сигнали для передачі даних.

- *Цифрова бездротова мережа*: Використовує цифрові сигнали для передачі даних і зазвичай є більш стійкою до спотворень.

- **За частотним діапазоном:**

- *WiFi (2.4 ГГц і 5 ГГц)*: Використовується для бездротового зв'язку в домашніх мережах і офісах.

- о *Bluetooth*: Використовується для з'єднання невеликих пристроїв в обмеженій області.

- о *4G/5G*: Мобільні мережі для передачі даних на великі відстані.

- о *Zigbee*: Використовується для IoT-пристроїв і має низьке споживання енергії.

- о *NFC (Near Field Communication)*: Використовується для короткодіючого обміну даними між пристроями на дуже близьких відстанях.

- **За призначенням:**

- о *Локальні бездротові мережі (Wireless Local Area Networks, WLANs)*: Використовуються для з'єднання пристроїв в межах обмеженої області, такої як офіс чи дім.

- о *Мобільні мережі*: Використовуються для забезпечення бездротового зв'язку між мобільними пристроями, такими як смартфони і планшети.

- о *Сенсорні мережі (Wireless Sensor Networks, WSNs)*: Використовуються для збору і передачі даних з сенсорів, розташованих у важкодоступних місцях.

10.3. Бездротові персональні мережі (WPAN)

Wireless Personal-Area Networks (WPAN) – бездротові персональні мережі – використовують малопотужні передавачі для мережі ближнього радіусу дії, зазвичай від 20 до 30 футів (від 6 до 9 метрів). WPAN засновані на стандарті 802.15 і використовують радіочастоту 2,4 ГГц.

10.3.1. Технологія IrDA

IrDA (Infrared Data Association) – це технологія бездротового зв'язку через інфрачервоні промені. Вона була розроблена для обміну даними між електронними пристроями, такими як комп'ютери, мобільні телефони, планшети, камери тощо, в недовідометрових відстанях.

IrDA використовує інфрачервоні промені для бездротового зв'язку. Ці промені не видимі для людського ока і використовуються для передачі даних шляхом модуляції світлового сигналу. IrDA працює у режимі точка-до-точки, що означає, що два пристрої повинні бути на пряму спрямовані один на одного для встановлення зв'язку. Це забезпечує високий рівень безпеки та уникнення нежаданих зв'язків. IrDA зазвичай підтримує високі швидкості

передачі даних, такі як 4 Мбіт/с та більше, що робить його придатним для великої кількості додатків, включаючи швидкий обмін файлами та друкування.

IrDA була широко використовуваною технологією для бездротового зв'язку в різних областях, таких як друкування, обмін контактами, синхронізація даних, керування віддаленими пристроями та інше. Дальність дії технології IrDA обмежена інфрачервоними променями і зазвичай становить кілька метрів. Прямий контакт та відсутність перешкод між пристроями є важливими факторами для стабільної роботи. З часом технологія IrDA стала менш популярною через зростання популярності інших бездротових технологій, таких як Bluetooth і Wi-Fi, які мають більший радіус дії та здатність працювати у більш різних умовах.

10.3.2. Технологія Bluetooth

Bluetooth – це бездротова технологія зв'язку, яка дозволяє пристроям обмінюватися даними на коротких відстанях (зазвичай в межах 10 метрів) через радіохвилі у короткому діапазоні. Технологія Bluetooth включає в себе наступні основні характеристики і переваги:

1. *Бездротовий зв'язок*: Bluetooth дозволяє пристроям підключатися один до одного без використання кабелів або проводів. Це надає зручність і портативність використання пристроїв.

2. *Короткі відстані*: Bluetooth розрахований на роботу на відносно невеликих відстанях, зазвичай в межах 10 метрів (залежно від версії Bluetooth і обставин).

3. *Широкий спектр застосувань*: Bluetooth використовується для підключення різних пристроїв, таких як гарнітури, клавіатури, миші, аудіосистеми, мобільні телефони, планшети, навушники, дрони, автомобільні системи та багато інших.

4. *Споживання енергії*: Bluetooth LE (Low Energy) або Bluetooth Smart - це версія Bluetooth, яка розроблена для пристроїв з низьким споживанням енергії, таких як сенсори для Інтернету речей (IoT) і фітнес-трекери. Вона дозволяє працювати на батареях довше.

5. *Широкий діапазон версій*: Bluetooth має кілька версій, включаючи Bluetooth 1.0, 2.0, 3.0, 4.0, 4.2, 5.0, 5.1 і 5.2, кожна з яких пропонує різні функції та покращення в сфері пропускну здатності, дальності та безпеки.

6. *Захищений зв'язок:* Bluetooth використовує протоколи шифрування для захисту передачі даних від несанкціонованого доступу.

7. *Простий процес парування:* Процес парування Bluetooth-пристроїв зазвичай досить простий і включає в себе взаємне визнання та підтвердження спільного підключення.

8. *Широка підтримка:* Bluetooth є стандартом, який підтримується більшістю сучасних мобільних пристроїв та комп'ютерів.

Технологія Bluetooth здійснює постійний розвиток, що розширює її можливості і застосування. Вона стала невід'ємною частиною багатьох аспектів нашого повсякденного життя і використовується в різних сферах, від розваг та спорту до медицини та автомобільних технологій.

10.3.3. Технологія зв'язку UWB

UWB, або *Ultra-Wideband*, є бездротовою технологією зв'язку, яка використовує велику ширину смуги для передачі даних на короткі відстані. Основні характеристики технології UWB включають:

1. *Велика ширина смуги:* UWB використовує дуже широкий діапазон радіочастот, що дозволяє передавати великі обсяги даних на високій швидкості. Ширина смуги UWB може бути від декількох сотень мегагерц до кількох гігагерц.

2. *Низька споживана потужність:* UWB зазвичай споживає менше енергії в порівнянні з іншими бездротовими технологіями, що робить її ідеальною для пристроїв з обмеженим джерелом живлення, таких як сенсори для Інтернету речей (IoT).

3. *Низькі електромагнітні впливи:* UWB має дуже короткі імпульси і велику ширину смуги, що дозволяє зменшити електромагнітні перешкоди та інтерференцію з іншими радіочастотними пристроями.

4. *Короткі відстані передачі:* Технологія UWB призначена для передачі даних на відносно короткі відстані, зазвичай до 10 метрів. Це робить її ідеальною для використання в бездротових пристроях, які знаходяться в непосредній близькості один від одного.

5. *Широкий спектр застосувань:* UWB використовується в різних сферах, включаючи медицину (наприклад, для вимірювання пульсу та дихання), автомобільну промисловість (наприклад, для систем позиціонування та безпеки), мілітарну технологію (наприклад, для з'єднання військових пристроїв) та інші галузі.

6. *Помірно короткий радіус дії*: У зв'язку з короткими відстанями передачі, UWB найбільш ефективно працює на відносно коротких відстанях, що обмежує її використання в додатках, де потрібно передавати дані на великі відстані.

Технологія UWB здобула популярність у багатьох галузях завдяки своїй високій швидкості передачі даних і низькому споживанню енергії, що робить її важливою для розвитку бездротових пристроїв та мереж.

10.3.4. Технологія зв'язку NFC

NFC (Near Field Communication, ближній радіозв'язок) – це короткодіюча бездротова технологія зв'язку, яка дозволяє пристроям обмінюватися даними на відстані до 10 сантиметрів один від одного. NFC створена для забезпечення швидкого та безпечного обміну інформацією між пристроями. Основні характеристики технології NFC включають:

1. *Короткодіюча дистанція*: NFC призначена для короткодіючого зв'язку на відстані до 10 сантиметрів. Це робить її ідеальною для обміну даними між пристроями, які знаходяться дуже близько один до одного.

2. *Споживання енергії*: NFC використовує низьку споживану потужність, що дозволяє працювати на батареях протягом тривалого часу. Це робить її популярною для бездротових платежів та інших застосувань.

3. *Простота використання*: Використання NFC дуже просте. Просто доторкніться одним пристроєм до іншого, і вони автоматично встановлюють підключення та обмінюються даними.

4. *Широкий спектр застосувань*: NFC використовується для бездротових платежів (наприклад, відомі послуги Apple Pay і Google Pay), обміну контактами, безпосереднього доступу до веб-сайтів, передачі фотографій та відео, забезпечення доступу до об'єктів (наприклад, вхід до готелю чи офісу) і багато інших сценаріїв.

5. *Безпека*: NFC має вбудовані механізми безпеки, які забезпечують конфіденційність та цілісність даних під час обміну. Також, зазвичай, для підтвердження платежів чи інших дій вимагається авторизація користувача (PIN-код, відбиток пальця тощо).

6. *Сумісність зі смартфонами*: Більшість сучасних смартфонів підтримують технологію NFC, що робить їх відмінними засобами для використання цієї технології.

NFC широко використовується в різних сферах, включаючи фінанси, маркетинг, туризм, безпеку та інші. Ця технологія відкриває двері до безконтактних платежів, спрощує обмін інформацією та робить багато різних аспектів життя більш зручними та ефективними.

10.4. Бездротові локальні мережі (WLAN)

Wireless LANs (WLAN) – бездротові локальні мережі - використовують передавачі для мережі середнього радіусу дії, як правило, до 300 футів (до 90 метрів). WLAN підходять для використання в будинку, офісі і навіть в кампусі. WLAN базуються на стандарті 802.11 і використовують радіочастоти 2,4 ГГц або 5 ГГц.

10.4.1. Огляд стандартів Wi-Fi

Стандарти IEEE 802.11 визначають технічні характеристики та протоколи для бездротових локальних мереж (WLAN). Основні стандарти IEEE 802.11 включають:

- *IEEE 802.11*: Це оригінальний стандарт, визначаючий основні принципи роботи бездротових локальних мереж. Він був прийнятий в 1997 році та працює на частоті 2.4 ГГц з можливістю передачі даних зі швидкістю до 2 Мбіт/с.
- *IEEE 802.11b*: Цей стандарт був прийнятий в 1999 році і використовує той же частотний діапазон, що і IEEE 802.11, але з підтримкою вищих швидкостей передачі даних (до 11 Мбіт/с).
- *IEEE 802.11a*: Прийнятий також в 1999 році, стандарт IEEE 802.11a використовує частотний діапазон 5 ГГц і підтримує швидкості передачі даних до 54 Мбіт/с. Він зазвичай забезпечує більшу пропускну здатність, але коротший радіус покриття порівняно з IEEE 802.11b.
- *IEEE 802.11g*: Цей стандарт, прийнятий у 2003 році, поєднує частотний діапазон IEEE 802.11b (2.4 ГГц) і швидкості передачі даних IEEE 802.11a (до 54 Мбіт/с).
- *IEEE 802.11n*: Прийнятий у 2009 році, стандарт IEEE 802.11n вдосконалив пропускну здатність і дальність покриття, підтримуючи технології, такі як MIMO (Multiple Input, Multiple Output). Швидкість передачі даних може сягати 600 Мбіт/с і більше.
- *IEEE 802.11ac*: Прийнятий у 2013 році, стандарт IEEE 802.11ac розширює пропускну здатність і покриття ще більше, підтримуючи

швидкості передачі даних до 1 Гбіт/с і більше. Він працює в частотному діапазоні 5 ГГц.

- *IEEE 802.11ax (Wi-Fi 6)*: Стандарт, прийнятий у 2019 році, пропонує ще більшу ефективність та пропускну здатність у бездротових мережах. Цей стандарт розроблений з огляду на зростаюче число підключених пристроїв IoT та вимоги до вищої пропускну здатності.

Кожен новий стандарт IEEE 802.11 вносить покращення у бездротові мережі, забезпечуючи більшу швидкість передачі даних, стабільність та забезпечуючи сумісність зі старішими стандартами для підтримки різноманітних пристроїв.

10.4.2. Методи побудови мереж WLAN

Побудова мережі WLAN (бездротової локальної мережі) включає в себе декілька методів і етапів. Етапи побудови мережі WLAN:

- *Вибір стандарту і технології*: Перший крок – це визначення стандарту бездротового зв'язку (наприклад, IEEE 802.11b/g/n/ac/ax) і технологій (наприклад, Wi-Fi) для вашої мережі. Вибір залежить від потреб і можливостей вашої організації.

- *Проектування мережі*: Ретельне проектування мережі WLAN включає в себе визначення місць розміщення точок доступу (AP), визначення потреби у пропускну здатності, розгортання системи безпеки (WPA, WPA2, WPA3), планування каналів і інші аспекти.

- *Розгортання AP*: Точки доступу (AP) розміщуються в приміщенні для покриття всієї області мережі бездротового зв'язку. При цьому слід враховувати фізичні перешкоди, такі як стіни і стелі.

- *Налаштування AP*: Кожна точка доступу налаштовується згідно з проектом мережі. Налаштування включають в себе ідентифікаційну інформацію мережі (SSID), безпеку, аутентифікацію і інші параметри.

- *Управління AP*: Управління AP може включати в себе моніторинг і відладку, а також оновлення програмного забезпечення і налаштування віддалено через централізоване програмне забезпечення управління мережею.

- *Встановлення мережеских налаштувань*: Крім AP, важливо правильно налаштувати шифрування, безпеку, керування доступом, канали і частоти, та інше.

Бездротові локальні мережі (WLAN) можуть бути побудовані різними методами, в залежності від конкретних потреб і обставин:

- **Інфраструктура з точкою доступу (Access Point, AP):**

- О Цей метод включає в себе встановлення одного або декількох точок доступу (AP) для обслуговування підключених пристроїв. Точки доступу зазвичай підключаються до провідної мережі і розміщуються в стратегічних точках для оптимального покриття.

- О Простий у встановленні та керуванні. Точки доступу зазвичай забезпечують додаткові функції, такі як шифрування і автентифікація для забезпечення безпеки.

- **Мережа Ad-hoc:**

- О У мережі Ad-hoc пристрої підключаються один до одного без використання центральної точки доступу. Примітно, що цей метод зазвичай використовується для створення бездротових мереж між пристроями, які знаходяться поруч.

- О Простий у налаштуванні, але не такий ефективний на великій площі і для багато пристроїв.

- **Mesh-мережі (Mesh Networks):**

- О Мережі з мережами – це метод побудови WLAN, при якому кожен пристрій може бути точкою доступу, яка підключена до інших пристроїв у мережі. Це створює резервне керування і забезпечує надійність та широкий радіус покриття.

- О Зазвичай використовується в мережах, де потрібно масштабувати покриття на великій площі або в складних умовах.

- **Спільноти користувачів (Community Networks):**

- О Цей метод передбачає об'єднання різних користувачів і пристроїв у спільну мережу. Це може бути використано для створення безкоштовних громадських мереж або спільнот, де користувачі надають доступ один одному через свої бездротові пристрої.

- **Каскадування точок доступу (Daisy Chaining):**

- О Цей метод використовується, коли потрібно підключити кілька точок доступу в одній мережі. Один AP підключається до іншого, створюючи послідовність AP.

- О Зручно для мереж з великою площею та обмеженим доступом до провідної мережі.

- **Гібридні підходи:**

- Іноді використовуються гібридні підходи, які комбінують різні методи побудови мереж WLAN в залежності від конкретних потреб і умов.

Вибір методу побудови мережі WLAN залежить від конкретних вимог до покриття, кількості підключених пристроїв, доступності провідної мережі та інших факторів.

10.4.3. Організація безпеки WLAN

Організація безпеки бездротової локальної мережі (WLAN) є критично важливою, оскільки бездротові мережі можуть бути уразливими для різних видів атак та несанкціонованого доступу. Основні кроки, які можна вжити для забезпечення безпеки мережі WLAN:

- **Використовуйте сильний пароль для мережі (PSK):**

- Встановіть надійний і складний пароль (WPA3-PSK) для доступу до мережі. Уникайте використання легких паролів і популярних фраз.

- **Виберіть надійний метод шифрування:**

- Використовуйте WPA3 або WPA2 з AES (Advanced Encryption Standard) для шифрування даних, що передаються в мережі. Уникайте застосування застарілих методів шифрування, таких як WEP, які є вразливими до взлому.

- **Змініть стандартні ідентифікатори (SSID):**

- Змініть стандартний SSID маршрутизатора або точки доступу на унікальний ідентифікатор. Використовуйте невідомий ідентифікатор, щоб ускладнити виявлення вашої мережі.

- **Використовуйте фільтр MAC-адреси:**

- Дозвольте доступ до мережі тільки пристроям, які мають дійсні MAC-адреси, які ви включили в список дозволених пристроїв.

- **Вимкніть WPS (Wi-Fi Protected Setup):**

- WPS може бути вразливим до атак, тому краще вимкнути цю функцію, якщо вона не потрібна.

- **Включіть гостьову мережу (Guest Network):**

- Якщо ваш маршрутизатор підтримує гостьову мережу, використовуйте її для ізоляції гостей від основної мережі. Встановіть обмежені права доступу для гостей.

- **Оновлюйте програмне забезпечення маршрутизатора:**

○ Регулярно оновлюйте програмне забезпечення маршрутизатора або точок доступу, оскільки оновлення часто включають у себе виправлення вразливостей.

- ***Змініть стандартні паролі адміністратора:***

○ Змініть стандартні паролі адміністратора маршрутизатора або точок доступу на складні та унікальні.

- ***Використовуйте відомі пристрої зі схваленими безпечними конфігураціями:***

○ Використовуйте пристрої з відомими та надійними безпечними конфігураціями для мережі.

- ***Моніторте мережу і аналізуйте журнали:***

○ Використовуйте програми для моніторингу мережі та аналізу журналів, щоб виявляти можливі атаки або незвичайну активність.

10.5. Бездротові міські мережі (WMAN)

Бездротові міські мережі (WMAN) – це тип бездротових мереж, які зазвичай покривають великі території міста або міські райони, надаючи доступ до Інтернету та інших мережевих послуг жителям та підприємствам. WMAN може бути використана для забезпечення доступу до Інтернету віддаленим районам, для підключення мобільних пристроїв, а також для впровадження різних послуг зв'язку.

Основні характеристики WMAN включають:

1. *Велика покриття:* WMAN має значно більше покриття, ніж бездротові локальні мережі (WLAN) і зазвичай охоплює територію міста або великих міських районів.

2. *Висока швидкість передачі даних:* WMAN може підтримувати високу швидкість передачі даних, що робить її ідеальною для використання у великих міських середовищах.

3. *Можливість передачі голосу, даних та відео:* WMAN може обслуговувати різні види трафіку, включаючи голосові дзвінки, передачу даних та відеострім.

4. *Підтримка різних стандартів:* WMAN може використовувати різні бездротові технології та стандарти, такі як WiMAX (Worldwide Interoperability for Microwave Access), LTE (Long-Term Evolution), 4G та 5G, для надання послуг.

5. *Складні технічні рішення:* Встановлення WMAN вимагає розгортання великої кількості антен, базових станцій і мережевого обладнання для забезпечення покриття та обслуговування клієнтів.

6. *Забезпечення якості обслуговування (QoS):* WMAN може використовувати техніки керування якістю обслуговування для забезпечення надійності та ефективності мережі.

WMAN може бути використана для різних застосувань, включаючи надання послуг Інтернету віддаленим районам, зв'язок для мобільних пристроїв у містах, підтримку міських систем моніторингу і контролю, телекомунікаційні послуги та багато інших сфер. WMAN грає важливу роль у покращенні доступу до зв'язку та Інтернету для населення та підприємств в міських середовищах.

10.6. Бездротові глобальні мережі (WWAN)

Бездротові глобальні мережі (WWAN) – це тип бездротових мереж, які надають послуги зв'язку на глобальному рівні, охоплюючи значну територію і надаючи зв'язок між різними регіонами, країнами та навіть континентами. WWAN використовує різні технології та стандарти, щоб забезпечити бездротовий доступ до Інтернету та інших послуг зв'язку в рухомому стані або в будь-якому місці, де є доступ до мережі WWAN.

10.6.1. Радіорелейний зв'язок

Радіорелейний зв'язок (microwave radio relay) є однією з технологій, що використовуються в бездротових глобальних мережах (WWAN) для передачі даних і забезпечення зв'язку на великі відстані. Радіорелейна мережа використовує радіохвилі, щоб передавати сигнали від одного пункту до іншого, і може бути дуже ефективною для створення бездротового зв'язку на значні відстані.

Основні характеристики радіорелейного зв'язку в WWAN включають:

- *Висока швидкість передачі даних:* Радіорелейна мережа зазвичай підтримує високу швидкість передачі даних, що дозволяє передавати великі обсяги інформації на великі відстані.
- *Велика відстань передачі:* Радіорелейний зв'язок дозволяє передавати сигнали на значні відстані, що робить його ідеальним для використання в WWAN, де потрібно забезпечити зв'язок на великій території.

- *Лінійний зв'язок*: Радіорелейні мережі часто працюють на принципі лінійного зв'язку, де сигнал передається від одного пункту до іншого через серію безпосередньо з'єднаних між собою станцій.

- *Низька затрата на встановлення і обслуговування*: В порівнянні з викладеними кабелями, радіорелейна мережа може бути менш коштовною у встановленні та обслуговуванні, оскільки вона не вимагає закладання фізичних ліній.

- *Повідомлення в реальному часі*: Радіорелейні мережі зазвичай надають можливість надсилати дані в режимі реального часу, що корисно для послуг, які вимагають низької затримки, таких як голосовий зв'язок і відеоконференції.

- *Стійкість до атмосферних впливів*: Радіорелейна мережа може працювати при поганих погодних умовах, хоча дощ, сніг та інші атмосферні явища можуть впливати на якість сигналу.

- *Низька затрата на передачу даних*: В порівнянні з іншими видами передачі даних, радіорелейний зв'язок може бути більш ефективним з точки зору витрат.

Радіорелейний зв'язок в WWAN використовується для забезпечення зв'язку між станціями та мережевими вузлами, що знаходяться на великій відстані один від одного.

Основні технічні характеристики радіорелейного зв'язку включають такі параметри:

- *Частота*: Частота радіосигналу, що використовується для передачі даних, є однією з важливих характеристик. Радіорелейні системи можуть використовувати різні діапазони частот, включаючи ультрависокі частоти (UHF), високі частоти (HF), мікрохвилі (SHF), купольні хвилі (EHF) та інші.

- *Ширина смуги (Bandwidth)*: Ширина смуги вказує на кількість частотного діапазону, який використовується для передачі сигналу. Широка смуга може підвищити пропускну спроможність мережі.

- *Потужність передавача (Transmit Power)*: Це вихідна потужність сигналу на стороні передавача. Вона вимірюється в ваттах або децибелах міліватт (dBm).

- *Чутливість приймача (Receiver Sensitivity)*: Це мінімальний рівень сигналу, який може бути прийнятий приймачем для успішної демодуляції та декодування. Вона вимірюється в децибелах міліватт (dBm).

- *Висота мачти або антени (Tower Height)*: Висота мачти або антени важлива для досягнення більшої дальності передачі та зниження впливу перешкод, таких як ліси, будівлі тощо.
- *Напрявленість антени (Antenna Gain)*: Це міра, як антена спрямовує сигнал у певному напрямку. Виражається в децибелах (dBi). Антени можуть бути напрямленими або омнідирективними (спрямовані в усі боки).
- *Модуляція і кодування (Modulation and Coding)*: Визначає спосіб, яким дані кодуються для передачі і як їх можна декодувати на приймачі. Висока модуляція дозволяє передавати дані з високою швидкістю, але може бути менш стійкою до помилок.
- *Затримка (Latency)*: Затримка вказує на час, який затрачається на передачу сигналу від передавача до приймача. Низька затримка важлива для додатків, які вимагають реального часу, наприклад, голосовий зв'язок та відеоконференції.
- *Мінімальна та максимальна відстань передачі*: Визначає максимальну відстань, на яку можна передавати сигнал із задовільною якістю прийому.
- *Модель поширення сигналу (Signal Propagation Model)*: Це математична модель, яка описує, як сигнал поширюється через повітря та які фактори впливають на якість зв'язку (наприклад, погода, рельєф місцевості тощо).

10.6.2. Супутникові технології

Супутникові технології грають важливу роль у бездротових глобальних мережах (WWAN), забезпечуючи зв'язок на великій відстані та в областях, де інші типи зв'язку можуть бути недоступними. Супутникові технології, які використовуються у WWAN, включають:

1. *Геостационарні супутники (Geostationary Satellites)*: Це супутники, які розташовані на висоті близько 35 786 кілометрів над екватором. Вони обертаються з такою швидкістю, що залишаються над певною точкою Землі, що дозволяє створювати стійкі точки зв'язку на великій відстані. Геостационарні супутники використовуються для послуг, таких як супутниковий Інтернет та міжнародний зв'язок.

2. *Низькоорбітальні супутники (Low Earth Orbit Satellites, LEO)*: Ці супутники розташовані на значно нижчій висоті, зазвичай від 160 до 2 000

кілометрів. Вони обертаються навколо Землі на високій швидкості і мають низьку затримку сигналу. Це робить їх ідеальними для послуги супутникового Інтернету та мобільного зв'язку, зокрема для регіонів, які не мають доступу до інших інфраструктурних засобів зв'язку.

3. *Середньоорбітальні супутники (Medium Earth Orbit Satellites, МЕО):* Це супутники, розташовані на висоті від 2 000 до 35 786 кілометрів. Вони забезпечують баланс між затримкою сигналу і покриттям. Середньоорбітальні супутники використовуються для послуг мобільного зв'язку та навігації, таких як GPS.

4. *Гібридні мережі:* Деякі WWAN мережі комбінують супутниковий зв'язок з іншими технологіями, такими як мережі на землі (наприклад, LTE або 5G). Це дозволяє отримати ширше покриття та підвищити доступність зв'язку.

5. *Супутникові телефони і термінали:* Для користувачів, які потребують мобільного зв'язку в віддалених або незвичайних умовах, існують супутникові телефони і термінали, які дозволяють підключатися до супутникових мереж та здійснювати голосовий зв'язок та передавати дані.

10.6.3. Технології передавання даних в стільникових мережах

Ці технології допомагають підвищити ефективність стільникових мереж і надають користувачам можливість отримувати доступ до широкого спектра послуг, включаючи голос, текст, мультимедійні дані і Інтернет, в будь-якому місці та в будь-який час.

- **GSM (Global System for Mobile Communications):** GSM був однією з перших технологій стільникового зв'язку і використовується для голосового зв'язку та передачі текстових повідомлень SMS. За допомогою GPRS (General Packet Radio Service) та EDGE (Enhanced Data Rates for GSM Evolution), GSM також здатен передавати дані, хоча з невеликою швидкістю.

- **3G (Third Generation):** 3G технології, такі як UMTS (Universal Mobile Telecommunications System) та CDMA2000, були розроблені для передачі великих обсягів даних з більшою швидкістю, що робить їх ідеальними для мобільного Інтернету, відеозвінків та інших послуг з високою швидкістю передачі даних.

- **4G LTE (Long-Term Evolution):** 4G LTE є наступним поколінням стільникових мереж і надає вищу швидкість передачі даних, низьку затримку і підтримку послуг з високою швидкістю, таких як стрімінг відео та

гігабітний Інтернет. Він також забезпечує покращену ефективність використання ресурсів мережі.

- **5G (Fifth Generation):** 5G - це найновіше покоління стільникових мереж, яке обіцяє надзвичайно високу швидкість передачі даних, низьку затримку і підтримку масового підключення IoT-пристроїв (Internet of Things). Воно має потенціал революціонізувати комунікації та підтримувати нові застосування, такі як автономні автомобілі та розширена віртуальна реальність.

- **Wi-Fi Offload:** Це технологія, яка дозволяє мобільним пристроям автоматично перемикатися зі стільникового зв'язку на Wi-Fi мережу, коли така мережа доступна. Це зменшує навантаження на стільниковий оператор і покращує якість обслуговування.

- **VoLTE (Voice over LTE):** VoLTE дозволяє передавати голосовий зв'язок через 4G LTE мережу, забезпечуючи кращу якість голосу і можливість одночасної передачі даних та голосу.

- **eSIM (Embedded SIM):** Ця технологія дозволяє віддалено активувати SIM-карту на мобільному пристрої без необхідності фізичної заміни SIM-карти. Це полегшує перехід між операторами та підключення до мережі.

10.7 Протоколи інтернету речей

Ці протоколи допомагають створювати різноманітні рішення для Інтернету речей, від смарт-дому і медичних пристроїв до міської інфраструктури та промислового обладнання. Вибір протоколу залежить від конкретних вимог проекту і типу пристроїв, які ви плануєте використовувати в вашій IoT-мережі.

- **MQTT (Message Queuing Telemetry Transport):** MQTT – це легкий та ефективний протокол спільноти, який призначений для передачі повідомлень між IoT-пристроями. Він використовує публікацію-підписку для організації комунікації між пристроями та серверами.

- **CoAP (Constrained Application Protocol):** CoAP – це протокол, розроблений спеціально для обмежених пристроїв та мереж Інтернету речей. Він дозволяє пристроям взаємодіяти через простий RESTful інтерфейс, що дозволяє виконувати операції, такі як отримання та оновлення даних. CoAP описаний в RFC 7252.

- **HTTP/HTTPS (Hypertext Transfer Protocol):** HTTP використовується для взаємодії між веб-програмами та пристроями Інтернету речей. За допомогою HTTP, пристрої можуть звертатися до веб-серверів для отримання та відправлення даних. HTTPS забезпечує захищену комунікацію через шифрування даних. HTTP і HTTPS описані в RFC 2616 та RFC 2818 відповідно.

- **DDS (Data Distribution Service):** DDS – це протокол для розподілу даних в реальному часі в IoT-мережах. Він дозволяє пристроям обмінюватися даними та керувати ними в реальному часі. DDS - це стандарт, який розробляє Object Management Group (OMG). Останній публічно доступний стандарт DDS називається "DDS for Real-Time Systems, Version 1.4".

- **Bluetooth:** Bluetooth стандарт використовується для безпроводової комунікації між близькорозташованими IoT-пристроями, такими як смартфони, сенсори та актуатори. Bluetooth LE (Low Energy) особливо підходить для батарейних пристроїв. Специфікації Bluetooth описані Bluetooth Special Interest Group (SIG). Номери версій можуть змінюватися. На момент останнього оновлення, актуальна версія - Bluetooth 5.2.

- **Zigbee:** Zigbee – це стандарт для мереж низької потужності, що дозволяє пристроям взаємодіяти в мережах Інтернету речей. Він широко використовується в додомових системах автоматизації. Останній стандарт Zigbee - Zigbee 3.0.

- **LoRaWAN (Long Range Wide Area Network):** LoRaWAN – це технологія бездротового зв'язку для далекого зв'язку IoT-пристроїв. Вона дозволяє відправляти дані на великі відстані, що робить її ідеальною для великих IoT-мереж. Останній стандарт - LoRaWAN 1.0.3.

- **NB-IoT (Narrowband Internet of Things):** NB-IoT – це стандарт для вузькосмугового зв'язку, призначений для великого обсягу IoT-пристроїв. Він працює в мережах стільникового зв'язку. NB-IoT описаний в документації від 3GPP (3rd Generation Partnership Project). Специфікація NB-IoT має кілька релізів, наприклад, NB-IoT Release 13.

- **Thread:** Thread – це стандарт для мереж Інтернету речей, розроблений для домашніх та комерційних застосувань. Він використовує протоколи IPv6 та 6LoWPAN для забезпечення комунікації. Thread описаний в специфікації Thread Group. Останній стандарт – Thread 1.1.

Контрольні запитання

1. Що таке бездротова мережа і які її основні переваги?
2. Назвіть різні типи бездротових мереж та їх призначення.
3. Які основні класифікації бездротових мереж існують?
4. Які стандарти бездротових мереж регулюються IEEE 802.11, і які їх характеристики?
5. Як працює технологія IrDA (Infrared Data Association) і для чого вона використовується?
6. Які основні принципи роботи технології Bluetooth і де її можна застосовувати?
7. Що таке WPAN (Wireless Personal Area Network) і які технології входять в цю категорію?
8. Як працює технологія UWB (Ultra-Wideband) і в яких сферах її використання найбільш актуальне?
9. Які основні аспекти технології NFC (Near Field Communication) і де її можна застосовувати?
10. Які методи побудови мереж WLAN (Wireless Local Area Network) використовуються для забезпечення бездротового зв'язку?
11. Які аспекти встановлення мережевих налаштувань важливі для правильної роботи бездротових мереж?
12. Які основні аспекти організації безпеки в бездротових мережах?
13. Що таке WMAN (Wireless Metropolitan Area Network) і які технології використовуються для побудови міських бездротових мереж?
14. Що таке WWAN (Wireless Wide Area Network) і які технології використовуються для глобального бездротового зв'язку?
15. Які технічні характеристики радіорелейного зв'язку важливі для WWAN?
16. Які технології передавання даних використовуються в стільникових мережах для забезпечення зв'язку між пристроями?
17. Які протоколи Інтернету речей (IoT) використовуються для забезпечення комунікації між IoT-пристроями?
18. Які номери стандартів протоколів Інтернету речей ви знаєте і де їх можна знайти?
19. Які технології передавання даних використовуються в мережах Інтернету речей?

РОЗДІЛ 11. ОГЛЯД КАТЕГОРІЙ АТАК НА КОМП'ЮТЕРНІ МЕРЕЖІ

11.1. Загальна характеристика та принципи організації системи безпеки

Ключовою характеристикою принципів організації системи безпеки є встановлення структурованого та комплексного підходу до захисту активів, інформації та осіб у певному середовищі. Ці принципи керують розробкою, впровадженням і керуванням системою безпеки, щоб забезпечити її ефективність у зменшенні ризиків, запобіганні несанкціонованому доступу та реагуванні на інциденти безпеки. Деякі ключові принципи організації системи безпеки включають:

- *Оцінка ризиків:* система безпеки повинна бути організована на основі ретельної оцінки потенційних ризиків і вразливостей. Виявлення загроз і встановлення пріоритетів допомагає належним чином розподілити ресурси та адаптувати заходи безпеки для вирішення конкретних завдань.
- *Рівневий захист:* добре організована система безпеки використовує кілька рівнів захисту. Цей підхід передбачає впровадження різноманітних заходів безпеки на різних рівнях для створення більш надійного та комплексного захисту від потенційних загроз.
- *Контроль доступу:* Контроль доступу до фізичних присторів, даних і систем має вирішальне значення. Організація системи безпеки повинна включати механізми керування та обмеження доступу на основі ролей, обов'язків та рівнів авторизації.
- *Моніторинг і спостереження.* Ефективні системи безпеки включають постійний моніторинг і спостереження. Це включає використання таких технологій, як камери, датчики та сигналізація, щоб виявляти підозрілі дії та реагувати на них у реальному часі.
- *Реагування на інциденти:* організована система безпеки містить чіткі процедури та протоколи для реагування на інциденти безпеки. Це включає кроки для оцінки ситуації, стримування загрози, пом'якшення впливу та ініціювання процесів відновлення.
- *Навчання та підвищення обізнаності:* люди в організації відіграють життєво важливу роль у забезпеченні безпеки. Принципи організації повинні включати навчальні програми для навчання співробітників найкращим практикам безпеки та підвищення обізнаності про потенційні ризики.

- *Регулярне тестування та оцінка:* системи безпеки необхідно регулярно тестувати, оцінювати та оновлювати для адаптації до нових загроз і технологій. Періодичні оцінки гарантують, що система залишається ефективною та дієвою.

- *Інтеграція та співпраця:* організована система безпеки має сприяти співпраці між різними відділами, такими як ІТ, управління об'єктами та кадрами, щоб забезпечити цілісний підхід до безпеки.

- *Відповідність і правила:* принципи організації мають передбачати дотримання відповідних законів, правил і галузевих стандартів. Забезпечення відповідності допомагає уникнути юридичних і нормативних проблем.

- *Постійне вдосконалення:* безпека – це постійний процес. Принципи організації повинні підкреслювати прагнення до безперервного вдосконалення, де уроки, отримані в результаті інцидентів і розвитку загроз, використовуються для вдосконалення та покращення системи безпеки.

11.2. Атаки доступу

Атаки доступу до комп'ютерних систем – це спроби несанкціонованого доступу до інформації, даних чи ресурсів комп'ютерної системи. Ці атаки можуть мати різні цілі, такі як крадіжка конфіденційних даних, порушення цілісності інформації, знищення даних, втручання у нормальне функціонування системи та інші.

Типи атак на доступ до комп'ютерних систем:

- ***Перехоплення даних (Sniffing):*** Атакуючі намагаються перехопити і аналізувати дані, що передаються по мережі, такі як паролі або конфіденційні інформаційні пакети.

- ***Атаки на паролі (Password Attacks):*** Включають методи, такі як перебір паролів, атаки за словником або використання шкідливих програм для отримання доступу до облікових записів користувачів.

- ***Фішинг (Phishing):*** Атакуючі намагаються обдурити користувачів і отримати від них конфіденційні дані, представляючись довіреними джерелами.

- ***Шкідливі програми (Malware):*** Це шкідливі програми, такі як віруси, хробаки, троянські коні та шпигунські програми, які можуть заразити комп'ютерну систему та діяти на шкоду її безпеці.

- **Відмова в обслуговуванні (Denial of Service, DoS):** Атакуючі створюють умови, за яких комп'ютерна система перевантажується та стає недоступною для легітимних користувачів.
- **Переповнення буфера (Buffer Overflow):** Атакуючі намагаються впровадити шкідливий код, переповнюючи буфер пам'яті програми та впливаючи на її нормальне виконання.
- **Атаки на вразливості (Vulnerability Exploits):** Ці атаки використовують відомі вразливості у програмному забезпеченні або операційній системі для отримання несанкціонованого доступу.
- **Атаки "людина посередині" (Man-in-the-Middle, MitM):** Атакуючі вставляються між двома сторонами, що комунікують, і перехоплюють або змінюють інформацію, що передається.



- **Соціальна інженерія (Social Engineering):** Атакуючі маніпулюють людьми, щоб отримати доступ до систем, використовуючи психологічні методи та обман.
- **Атаки на мережеві служби (Service Attacks):** Включають атаки на служби, що працюють на серверах, такі як атаки на веб-додатки, DNS-атаки та інші.

11.3. Атаки модифікації

Атаки модифікації відносяться до типу кіберзлочинності, де зловмисники намагаються змінити чи підробити дані, файли, програми, або інші елементи в системі з метою завдання шкоди, отримання незаконного доступу, або введення в оману користувачів. Ці атаки можуть бути

спрямовані на порушення цілісності, конфіденційності, або доступності даних та ресурсів.

Деякі типи атак модифікації:

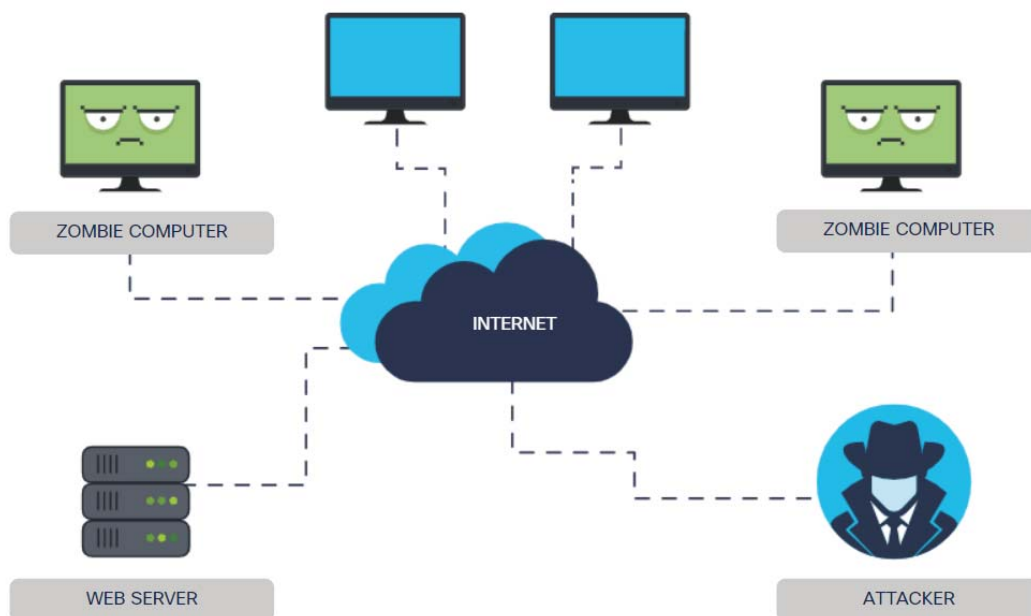
- **Внесення змін в дані:** Зловмисники можуть змінювати дані в системах або базах даних, щоб спотворити інформацію, викликати плутанину, або ввести в оману користувачів.
- **Підробка файлів:** Зловмисники можуть підробити файли, наприклад, додавши шкідливий код до виконуваних файлів, документів або мультимедійних матеріалів.
- **Зміна конфігурацій:** Атаки можуть включати зміну налаштувань системи, програм або мереж для порушення їх звичайної роботи або використання в злочинних цілях.
- **Введення шкідливих даних:** Зловмисники можуть намагатися внести шкідливі дані або команди в систему, які можуть використовуватися для злому або підбурювання інших атак.
- **Зміна пересилання:** Ця атака полягає в зміні спрямувань комунікації між системами, щоб перехопити або модифікувати дані, які передаються між ними.
- **Фальшиві оновлення:** Зловмисники можуть створити фальшиві оновлення або підробити патчі для програмного забезпечення з метою введення шкідливого коду.
- **Зміна даних у транзакціях:** В атаках на фінансові системи можуть змінювати дані у фінансових транзакціях для отримання незаконних вигод.
- **Маніпуляція API:** Зміна або підробка запитів та відповідей API може використовуватися для отримання доступу до даних або систем.

Запобігання атакам модифікації включає в себе використання криптографічних методів для забезпечення цілісності даних, застосування контролю доступу, використання безпечних засобів зберігання і передачі даних, а також регулярне оновлення та моніторинг системи для виявлення незвичайних змін.

11.4. Атаки на відмову в обслуговуванні

Атаки на відмову в обслуговуванні (Distributed Denial of Service або DDoS) – це тип кібератак, при якому зловмисники намагаються переповнити цільовий об'єкт (наприклад, веб-сайт, сервер або мережу) великим обсягом

запитів або трафіку, з метою зробити його недоступним для легітимних користувачів.



Головна мета атак DDoS – перевантажити ресурси цільової системи або мережі, таким чином, щоб вона не змогла нормально обслуговувати запити користувачів. Така атака може спричинити відмову доступу до сервісів, порушення роботи веб-сайту або навіть призвести до тимчасового припинення роботи цілої мережі.

Існують різні типи DDoS-атак:

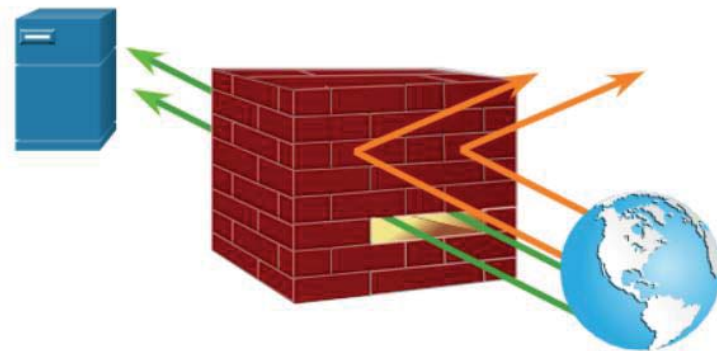
- **Атаки з використанням ботнетів:** Зловмисники використовують мережі комп'ютерів, які підконтрольовані їм (ботнети), для відправки великої кількості запитів на цільовий об'єкт.
- **Ампліфікаційні атаки:** Зловмисники використовують публічні послуги, які можуть генерувати велику відповідь на невеликий запит (наприклад, DNS або NTP сервери), для посилення обсягу трафіку, який направляється на цільовий об'єкт.
- **Синхронізаційні атаки:** Зловмисники намагаються витратити ресурси цільової системи, викликавши додаткові витрати обчислювальної потужності для обробки запитів.
- **Slowloris атаки:** Зловмисники намагаються витратити всі доступні з'єднання до цільового сервера, відкриваючи багато недокінцевих з'єднань із повільною передачею даних.

Запобігання атакам DDoS включає в себе використання спеціального обладнання та програмного забезпечення для виявлення та фільтрації

шкідливого трафіку, розробку планів відновлення після атаки, а також підтримку масштабованої інфраструктури для витримки великого обсягу трафіку.

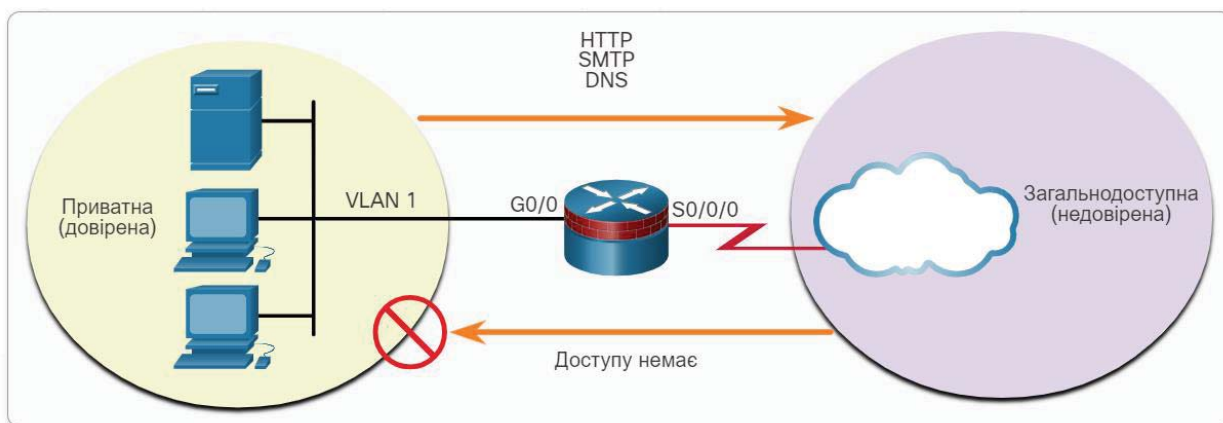
11.5. Захист мережі з використанням брандмауерів

Брандмауери є важливою складовою засобу захисту комп'ютерних мереж від небажаних доступів, загроз та атак. Вони допомагають контролювати і регулювати потік даних між комп'ютерами або мережами з різних сторін інтернету, а також внутрішніми мережами організації.



Основні функції брандмауера включають:

- *Фільтрація трафіку:* Брандмауер може фільтрувати вхідний та вихідний мережевий трафік залежно від правил та параметрів налаштувань. Це дозволяє блокувати шкідливий трафік та незаконний доступ.
- *Доступ до ресурсів:* Брандмауер може контролювати доступ до різних ресурсів мережі, таких як сервери, служби, файли тощо, на основі різних критеріїв, наприклад, IP-адрес, портів, протоколів тощо.
- *Перенаправлення портів:* Брандмауер може використовуватися для перенаправлення мережевого трафіку з одного порту на інший, що може бути корисним для розподілення навантаження або віддаленого доступу до ресурсів.
- *Виявлення та запобігання інтрузіям:* Багато сучасних брандмауерів мають функції виявлення та запобігання інтрузіям (Intrusion Detection and Prevention System, IDS/IPS), які спрямовані на виявлення та блокування вторгнень у мережу.
- *VPN тунелювання:* Брандмауер може підтримувати створення зашифрованих VPN-з'єднань, що забезпечують безпечний доступ до мережі з віддалених місць.



Для ефективного захисту мережі з використанням брандмауера рекомендується виконати наступні кроки:

- *Вибір відповідного брандмауера:* Виберіть брандмауер, який найкраще підходить для вашої організації. Це може бути апаратний брандмауер, програмний брандмауер або хмарний брандмауер.
- *Встановлення та налаштування:* Встановіть брандмауер у мережу та правильно налаштуйте його параметри. Визначте правила доступу, фільтрації трафіку, перенаправлення портів тощо.
- *Оновлення та моніторинг:* Регулярно оновлюйте програмне забезпечення брандмауера, щоб забезпечити захист від нових загроз. Ведіть моніторинг мережі та брандмауера для виявлення незвичайної активності.
- *Використання IDS/IPS:* Якщо брандмауер підтримує IDS/IPS, налаштуйте ці функції для виявлення та блокування інтрузій.
- *Використання VPN:* Якщо це потрібно, налаштуйте зашифровані VPN-з'єднання для безпечного доступу до мережі.
- *Регулярні аудити та тестування:* Періодично проводьте аудити безпеки та тестування, щоб переконатися в ефективності брандмауера та знайти можливі слабкі місця.

Важливо розбиратися в різних типах брандмауерів та їхніх специфічних можливостях, щоб для кожної ситуації використовувався правильний брандмауер.

Брандмауер з фільтруванням пакетів (без врахування стану)

Брандмауер з фільтруванням пакетів зазвичай є частиною брандмауера-маршрутизатора, що дозволяє або забороняє трафік на основі інформації Рівнів 3 і 4. Це міжмережні екрани без врахування стану, які використовують простий пошук по таблиці політик та фільтрують трафік за певними критеріями.

Наприклад, сервери SMTP за замовчуванням прослуховують порт 25. Адміністратор може налаштувати брандмауер фільтрування пакетів, щоб заблокувати порт 25 з певної робочої станції, для запобігання передачі вірусу електронною поштою.

Брандмауер зі збереженням стану

Брандмауери зі збереженням стану є найбільш універсальними та найпоширенішими технологіями брандмауера, що використовуються. Брандмауери зі збереженням стану забезпечують фільтрування пакетів через стан, використовуючи інформацію про з'єднання, що зберігається в таблиці стану. Фільтрація зі збереженням стану – це архітектура брандмауера, яка застосовується на мережному рівні. Вона також аналізує трафік на Рівнях 4 та 5 OSI.

Брандмауер шлюзу застосунків

Брандмауер шлюзу застосунків (брандмауер проксі) фільтрує інформацію на Рівнях 3, 4, 5 та 7 еталонної моделі OSI. Більша частина контролю і фільтрації в брандмауері виконується програмним забезпеченням. Коли клієнт повинен отримати доступ до віддаленого сервера, він під'єднується до проксі-сервера. Проксі-сервер під'єднується до віддаленого сервера від імені клієнта. Тому сервер бачить лише з'єднання з проксі-сервером.

Брандмауер наступного покоління

Брандмауери наступного покоління (NGFW, Next-generation firewalls) – це міжмережний екран зі збереженням стану, який має розширений функціонал, що забезпечує:

- Комплексний захист від вторгнень
- Поінформованість про застосунки та керування ними для перегляду і блокування ризикованих програм
- Шляхи оновлення для включення майбутніх інформаційних потоків
- Методи боротьби з загрозами безпеки, що розвиваються

Контрольні питання

1. Що таке брандмауери і які їхні основні функції у захисті комп'ютерних мереж?

2. Які види атак можуть бути відповідно здолані за допомогою брандмауерів?
3. Які можливості забезпечує фільтрація трафіку брандмауера?
4. Як брандмауери можуть регулювати доступ до ресурсів в мережі?
5. Що таке IDS/IPS і як вони можуть бути використані у контексті брандмауерів?
6. Які фактори варто враховувати при виборі відповідного брандмауера для організації?
7. Які кроки рекомендується виконати для належного налаштування брандмауера та забезпечення його ефективної роботи?
8. Чому важливо регулярно оновлювати програмне забезпечення брандмауера?
9. Які переваги має використання VPN з брандмауером для безпечного доступу до мережі?
10. Які додаткові кроки можуть бути вжиті для забезпечення безпеки мережі, окрім використання брандмауера?

РОЗДІЛ 12. МЕТОДИ ЗДІЙСНЕННЯ АТАК НА ІНФОРМАЦІЙНІ МЕРЕЖЕВІ СИСТЕМИ

12.1. DoS-атаки

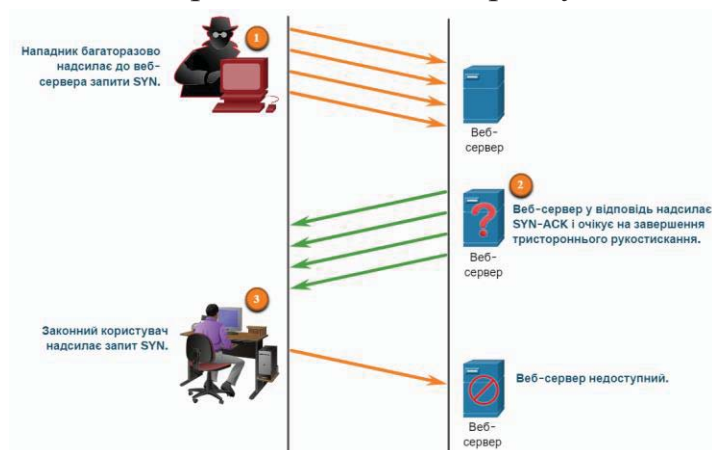
Атаки типу "Denial of Service" (DoS) спрямовані на перевантаження ресурсів системи або мережі, з метою заборонити легітимним користувачам отримання доступу до цих ресурсів. Це може включати доступ до веб-сайту, мережевого сервісу, сервера, мережевого елементу тощо.

Методи здійснення DoS атак:

Надмірне навантаження (Traffic Overload):

- **TCP SYN Flood:** Зловмисник відправляє багато підроблених запитів SYN на сервер, не завершуючи їхню ініціацію, що призводить до вичерпання ресурсів сервера.

Для проведення лавинних атак із застосуванням TCP SYN або SYN-флуд (TCP SYN Flood) використовуються особливості тристороннього рукошестискання TCP. На рисунку зображений нападник, який безперервно надсилає до вузла-жертви пакети TCP SYN із запитом на відкриття сеансу, що містять підроблену випадкову IP-адресу відправника. Цільовий пристрій відповідає на вказану фіктивну IP-адресу пакетом TCP SYN-ACK і чекає на отримання TCP ACK. Ці відповіді ніколи не надходять. Зрештою, цільовий вузол переобтяжується надмірною кількістю напіввідкритих TCP-з'єднань і відмовляє у наданні TCP-сервісів законним користувачам.



- **UDP Flood:** UDP не забезпечує захисту за допомогою шифрування. Функції шифрування можна додати до протоколу UDP, проте за замовчуванням вони недоступні. Відсутність шифрування дозволяє будь-

кому переглядати трафік, змінювати його та надсилати за призначенням. Зміна даних в трафіку викликає зміну 16-бітної контрольної суми, яка є необов'язковою і не завжди використовується. Якщо її все ж беруть до уваги, зломисник може створити нове значення контрольної суми на основі оновленого корисного навантаження і записати його у заголовок. Пристрій призначення виявить, що контрольна сума відповідає даним, не підозрюючи про внесені зміни. Цей тип атаки не дуже широко поширений.

Більш ймовірно, що вам зустрінеться лавиноподібна атака з використанням UDP. Лавиноподібні атаки UDP або UDP-флуд (UDP flood) спрямовані на виснаження усіх ресурсів мережі. Для цього зломиснику потрібно використовувати такі інструменти, як UDP Unicorn або Low Orbit Ion Cannon. Ці засоби скеровують на сервер у підмережі лавину UDP-пакетів, найчастіше, з підроблених вузлів. Програма перегляне усі відомі порти, намагаючись виявити серед них закриті. В результаті, на кожен такий запит сервер відповідатиме ICMP-повідомленням про недоступність порту. Оскільки на сервері існує безліч закритих портів, в результаті в сегменті виявляється настільки великий обсяг трафіку, що використовується майже вся смуга пропускання. Досягнутий ефект дуже схожий на DoS-атаку.

Засмічування ресурсів (Resource Exhaustion):

- *HTTP Flood:* Відправка великої кількості запитів HTTP на веб-сайт, перевантажуючи сервер та забороняючи доступ легітимним користувачам.
- *Ping Flood:* Відправка великої кількості пакетів ICMP ping на цільовий пристрій, що може призвести до відмови в обслуговуванні.
-

Ампліфікація (Amplification):

- *DNS Amplification:* Зломисник відправляє запити до відкритих DNS-серверів зі спуфікованою адресою цільової жертви, що призводить до великого обсягу відповідей, спрямованих на жертву.
- *NTP Amplification:* Зломисник використовує Network Time Protocol (NTP) сервери для відправки великої кількості запитів на жертву.

Синхронізація ресурсів (Resource Synchronization):

- *Смартфон-ампліфікація (Smartphone Amplification):* Використання масового співробітництва багатьох пристроїв (наприклад, смартфонів) для одночасного відправлення запитів на цільовий ресурс.

Програмні вразливості (Software Vulnerabilities):

- **Zero-Day Exploits:** Використання невідомих раніше уразливостей в програмному забезпеченні, що може призвести до відмови в обслуговуванні або відмови в роботі.

Довідкові атаки (Reflection Attacks):

- **Синхронізація (Reflection):** Використання протоколів або сервісів, що дозволяють використання відповідей в якості запитів для заборони обслуговування на цільовому сервері.

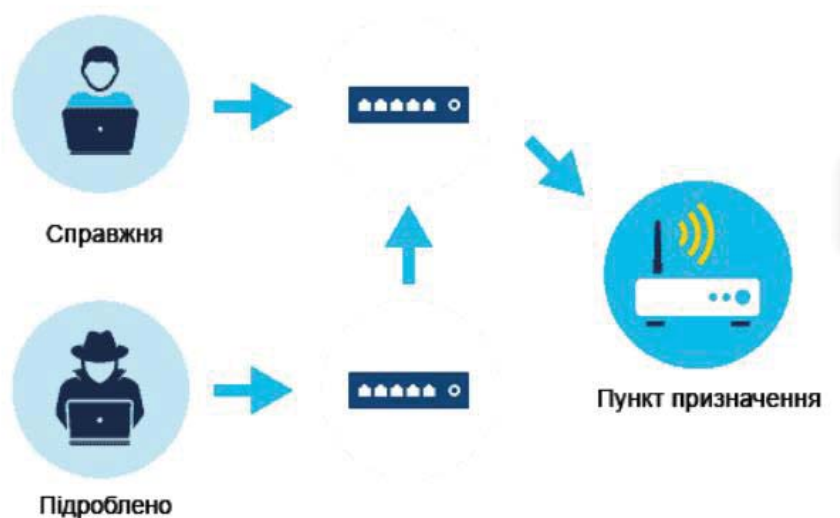
12.2. Прослуховування комутованих мереж (сніфінг)

Сніфінг (англ. "sniffing") або прослуховування комутованих мереж - це метод атаки на інформаційні мережеві системи, під час якого зломисник спробує отримати доступ до незашифрованих даних, які передаються по мережі. Це може включати конфіденційну інформацію, яку відправляють або отримують користувачі, таку як паролі, особисті дані, фінансова інформація тощо.

Методи здійснення атаки сніфінгу:

- ***ARP Poisoning (ARP Spoofing):***

Зломисник відправляє фальшиві повідомлення ARP (Address Resolution Protocol) на мережу, щоб вказати, що його MAC-адреса відповідає IP-адресі жертви. Це дозволяє зломиснику перехоплювати трафік, призначений для жертви.



- **MAC Flooding:**

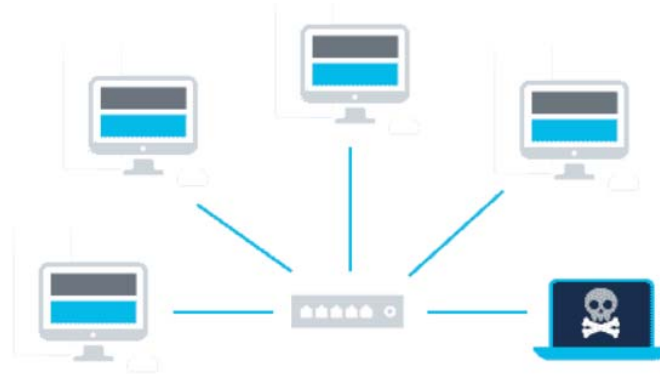
Зловмисник заповнює кеш MAC-адресів комутатора великою кількістю фальшивих записів, що призводить до того, що комутатор переходить у режим "багатокастового" розсилання пакетів, а не розсилає їх лише до відповідних портів.

- **Packet Sniffing Tools:**

Зловмисник використовує спеціальні програми для перехоплення трафіку, що проходить через мережеві інтерфейси. Такі програми можуть зчитувати та відображати дані, які передаються по мережі.

- **Hub-based Networks:**

У мережах на базі хабів, весь трафік розсилається на всі порти, що дозволяє зловмиснику підключитись до мережі та перехоплювати трафік, адресований іншим користувачам.



- **Malicious Software:**

Зловмисник може використовувати шкідливе програмне забезпечення, таке як віруси, троянські програми або "шпигуни", для перехоплення і передачі даних з інфікованих систем.

- **Switch Port Mirroring (SPAN):**

У деяких випадках, зловмисники можуть використовувати можливість "дзеркального відображення порта" на комутаторах, щоб отримати доступ до всього трафіку, що проходить через вибраний порт.

Для захисту від атаки сніфінгу рекомендується використовувати захищені протоколи передачі даних, шифрування трафіку, встановлення мережевих брандмауерів та систем виявлення вторгнень, а також використання комутаторів з підтримкою функцій безпеки.

12.3. Імітація IP-адреси (IP-спуфінг)

Атака імітації IP-адреси (IP-спуфінг) полягає в тому, що зловмисник намагається надати пакетам підроблений або іншим чином фальсифікований IP-адресування, щоб обдурити приймаючий пристрій чи сервер та викликати певні негативні реакції або вразити інші аспекти мережевої безпеки.

Методи здійснення атаки імітації IP-адреси:

- ***Smurf Attack:***

Зловмисник відправляє велику кількість ICMP Echo Request пакетів (ping) з підробленим IP-адресою жертви на широкомовну адресу мережі. Відповіді на ці запити, назад до жертви, можуть призвести до перевантаження її ресурсів.

- ***Spoofed TCP/IP Packets:***

Зловмисник може відправляти підроблені TCP або UDP пакети зі спуфікованим IP-адресою. Це може призвести до підробки сесій, аутентифікації чи навіть розриву зв'язку між легітимними пристроями.

- ***Man-in-the-Middle (MitM) Attack:***

Атака "людина в середині" може включати підробку IP-адреси для створення фальшивого зв'язку між двома легітимними пристроями, при цьому зловмисник перехоплює та контролює передачу даних між ними.

- ***DNS Spoofing:***

Зловмисник може використовувати IP-спуфінг для підробки DNS-записів, вказуючи на власні фальшиві IP-адреси. Це може призвести до переадресації легітимних запитів до фальшивих сторінок або серверів.

- ***Application-Level Attacks:***

В деяких випадках зловмисник може підробити IP-адресу в заголовку додаткових даних додатків, що може призвести до обману або порушення роботи додатків.

- ***ARP Spoofing:***

Ця атака, згадана раніше, також може бути вважана атакою імітації IP-адреси, оскільки ARP відповідає за відображення IP-адрес на MAC-адресу.

Для захисту від атак імітації IP-адреси рекомендується використовувати протоколи аутентифікації та шифрування, контролювати та фільтрувати мережевий трафік, використовувати протоколи безпеки на різних рівнях мережі та застосовувати відповідні політики безпеки на всіх рівнях інфраструктури.

12.4. Ін'єкції

Атаки ін'єкцій полягають в тому, що зловмисник вводить шкідливий код, дані чи команди в вразливі компоненти або програми, які обробляють дані, що надходять від користувачів. Це може призвести до виконання небажаного коду, розкриття конфіденційних даних або порушення роботи системи.

Методи здійснення атак ін'єкцій:

- ***SQL Injection (SQLi):***

Зловмисник вводить SQL-код у веб-форми або параметри запитів, які передаються до бази даних. Це може призвести до незаконного доступу до бази даних, розкриття конфіденційних даних або зміни даних в базі.

- ***Cross-Site Scripting (XSS):***

Зловмисник вводить скрипти (наприклад, JavaScript) у веб-сторінки або дані, які передаються на браузер користувача. Це може призвести до виконання небажаного коду на боці користувача, крадіжки куки-файлів або виконання дій в контексті вразливого додатку.

- ***Command Injection:***

Зловмисник вводить команди або системні виклики в веб-форми або інші ввідні поля. Це може дозволити виконання шкідливих команд на сервері.

- ***XML Injection:***

Зловмисник вводить зловісні дані в XML-структури, що оброблюються додатками. Це може призвести до розкриття конфіденційних даних або зловмисного впливу на обробку XML-даних.

- ***LDAP Injection:***

Зловмисник вводить зловісні дані в LDAP-запити, які використовуються для пошуку даних у каталогах. Це може призвести до витoku конфіденційної інформації або незаконного доступу до даних.

- ***Code Injection:***

Зловмисник вводить вразливий код, який виконується на сервері. Це може призвести до виконання шкідливого коду або зміни поведінки додатку.

- ***OS Commanding:***

Зловмисник вводить системні команди для виконання на операційній системі сервера. Це може призвести до виконання небажаного коду або отримання доступу до системи.

Захист від атак ін'єкцій включає в себе валідацію та санітизацію вхідних даних, використання параметризованих запитів до бази даних,

належну конфігурацію безпеки серверів та додатків, а також використання спеціалізованих інструментів для виявлення і ліквідації вразливостей.

12.5. Соціальний інжиніринг

Соціальний інжиніринг – це метод атаки, в якому зловмисники використовують психологічні маніпуляції та маніпулюють довір'ям користувачів для отримання конфіденційної інформації, доступу до системи або виконання певних дій. Основний аспект цієї атаки полягає у тому, що зловмисник впливає на людей, щоб ті вчинили небажані дії без підозрі або недоліків.

Методи здійснення атаки соціального інжинірингу:

- ***Фишинг (Phishing):***

Відправка шахрайських електронних листів або повідомлень, що виглядають як легітимні комунікації від організацій, банків або інших джерел. Ці повідомлення можуть містити посилання на фальшиві веб-сайти або запити ввести конфіденційну інформацію.

- ***Спішка (Pretexting):***

Зловмисник вигадує історію або піддурюється під якусь авторитетну особу, щоб переконати людей виконати певні дії. Наприклад, звертатися до служби підтримки та вигадувати проблеми для отримання конфіденційної інформації.

- ***Відволікання (Distraction):***

Зловмисник створює ситуацію, що відволікає увагу людей, під час якої він може виконати небажані дії, наприклад, отримати доступ до комп'ютера або документів.

- ***Техніка "Найкращий друг" (Best Friend):***

Зловмисник вигадується під довірливого або знайомого людину та просить допомогти з важливим питанням, таким чином здобуваючи конфіденційну інформацію.

- ***Техніка "Подарунок" (Gift Giving):***

Зловмисник може намагатися отримати доступ або інформацію, пропонуючи подарунки або обіцянки вигоди.

- ***Викрадання ідентичності (Identity Theft):***

Зловмисник вивчає інформацію про цільову особу та використовує її ідентичність для доступу до системи або виконання шахрайських дій.

- **У хвості (Tailgating):**

Зловмисник використовує тактику просування разом з внутрішньою особою або використовує її доступ для отримання доступу до заборонених областей.

- **Соціальні мережі (Social Media):**

Зловмисник використовує інформацію, розміщену на соціальних мережах, для вигадування впливових історій та впливу на цільових осіб.

Для захисту від атак соціального інжинірингу, користувачам слід бути обережними та освіченими щодо можливих загроз. Регулярна освіта з питань кібербезпеки, дотримання строгих політик безпеки, використання двофакторної аутентифікації та заборона видачі конфіденційної інформації без належної перевірки можуть допомогти запобігти успішним атакам соціального інжинірингу.

Контрольні питання

1. Що таке атака типу "Denial of Service" (DoS) і яка її мета?
2. Наведіть приклади методів здійснення DoS атак.
3. Які методи можуть бути використані для захисту від атак DoS?
4. Що таке атака "прослуховування комутованих мереж (сніфінг)" і чому вона небезпечна?
5. Перерахуйте декілька методів здійснення атаки сніфінгу.
6. Які заходи можна вжити для запобігання атакам сніфінгу?
7. Що таке атака "Імітація IP-адреси (IP-спуфінг)" і яка її основна мета?
8. Назвіть декілька методів здійснення атаки імітації IP-адреси.
9. Які кроки можна вжити для зменшення ризику атаки імітації IP-адреси?
10. Що таке атака "Ін'єкції" і які її можливі наслідки?
11. Приведіть приклади атак ін'єкцій та способи їх попередження.
12. Що таке атака "Соціальний інжиніринг" і яким чином зловмисники використовують психологічні маніпуляції?
13. Назвіть декілька методів здійснення атаки соціального інжинірингу.
14. Які кроки можна підприйняти для зменшення вразливості перед атаками соціального інжинірингу?

РОЗДІЛ 13. СТАНДАРТИ МЕТОДІВ І ЗАСОБІВ ЗАХИСТУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ

13.1. Побудова моделей порушника й атак на комп'ютерні мережі та системи

13.1.1. Аналіз умов функціонування та сучасних загроз інформації в комп'ютерних мережах та системах

Аналіз умов функціонування локальних і глобальних обчислювальних систем показав, що головною вимогою, яка висувається до них, є забезпечення користувачам потенційної можливості доступу до поділюваних ресурсів усіх комп'ютерів, об'єднаних у мережу [10; 19; 21 – 24; 41 – 42; 47; 49 – 51].

До основних вимог функціонування глобальних обчислювальних систем (ГОС) відносяться: продуктивність, надійність, сумісність, керованість, захищеність, розширюваність і масштабованість. Основні вимоги і їх складові наведені на рис. 13.1.

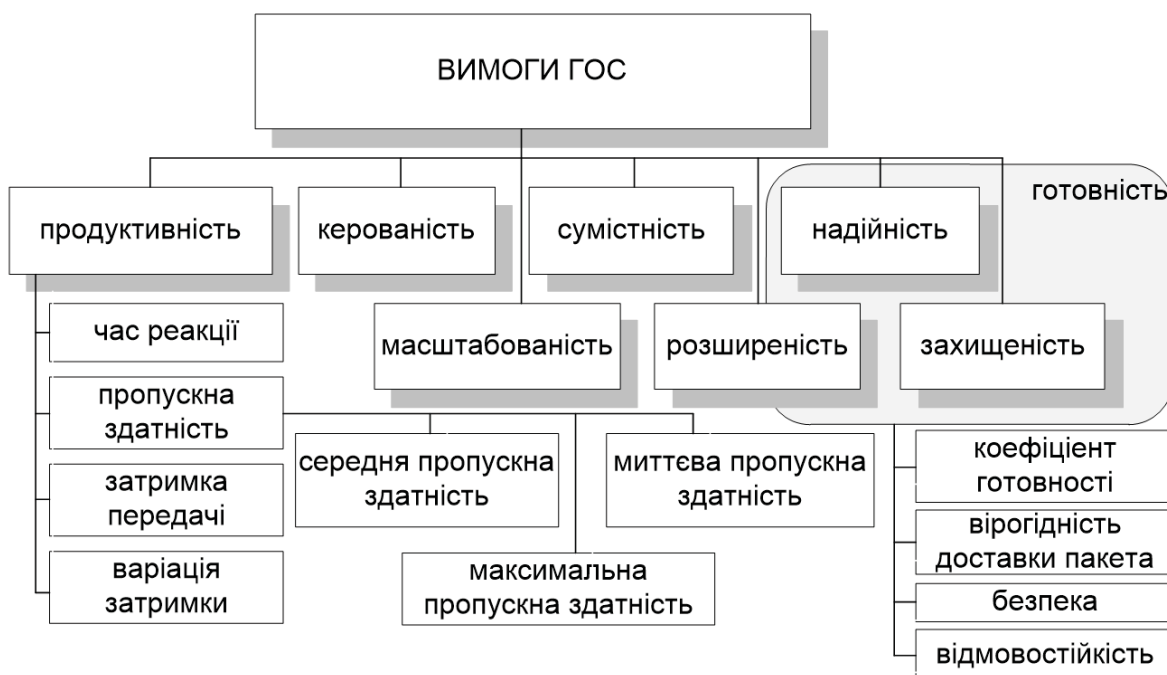


Рис. 13.1. Вимоги, які висуваються до обчислювальних мереж та систем

У даний час для оцінки функціонування локальних обчислювальних систем (ЛОС) і ГОС введено поняття “якість обслуговування” (Quality of Service, QoS) комп’ютерної мережі, що включає тільки дві найважливіші характеристики – продуктивність і надійність [36; 42; 46].

Проведений аналіз показника якості обслуговування мережі визначає два підходи до його забезпечення [36; 42; 46].

Перший підхід полягає в гарантованому забезпеченні користувачу дотримання деякої числової величини показника якості обслуговування (забезпечення встановленого показника середньої пропускної здатності, показника часу затримки передачі і т. д.). Так, наприклад, технології Frame Relay і АТМ дозволяють будувати мережі, що гарантують якість обслуговування за продуктивністю (показники середньої пропускної здатності, часу реакції, часу затримки та ін.).

Другий підхід полягає в пріоритетному обслуговуванні користувачів відповідно до встановленої ієрархії мережі. Таким чином, якість обслуговування залежить від ступеня привілейованості користувача або групи користувачів, до якої він належить. Для вповноважених користувачів ГОС якість обслуговування не гарантується, а гарантується тільки рівень їх привілеїв. Таке обслуговування називається обслуговуванням best effort – з найбільшим старанням. Проведений аналіз функціонування локальних мереж показує, що за таким принципом працюють ЛОС, побудовані на комутаторах з пріоритетом кадрів.

Для забезпечення необхідного показника якості обслуговування ГОС необхідно забезпечити продуктивність і надійність. Під продуктивністю [15; 36; 42; 46] розуміється властивість, що забезпечує можливість розпаралелювання робіт між декількома комп’ютерами мережі.

Основними характеристиками продуктивності є: час реакції, пропускна здатність, затримка передачі і її варіація.

Час реакції [15; 46] є інтегральною характеристикою продуктивності мережі й визначається як інтервал часу між виникненням запиту користувача до якої-небудь мережної служби й одержанням відповіді на цей запит.

Проведений аналіз даного показника показує, що його значення залежить тільки від типу служби, до якої звертається користувач, статусу користувача в мережі, типу сервера, а також від поточного стану елементів ГОС – завантаженості сегментів, комутаторів і маршрутизаторів, через які проходить запит, завантаженості сервера та ін.

Час реакції мережі розподіляється на час підготовки запитів на клієнтському комп'ютері, час передачі запитів між клієнтом і сервером через комунікаційне встаткування, час обробки запитів на сервері, час передачі відповідей від сервера клієнту і час обробки одержуваних від сервера відповідей на клієнтському комп'ютері.

Для визначення обсягу переданих даних за одиницю часу використовується пропускна здатність та її похідні (миттєва, максимальна і середня пропускні здатності).

При цьому середня пропускна здатність [15; 46] визначається як співвідношення загального обсягу переданих даних до часу їх передачі за тривалий проміжок часу (доба, місяць, рік), миттєва пропускна здатність [15; 36; 42; 46] визначається за дуже маленький проміжок часу (від 0,1 до 10^{-3} с) і максимальна пропускна здатність визначається як найбільша миттєва пропускна здатність, зафіксована протягом періоду спостереження.

Аналіз функціонування ГОС показує, що для проектування, налаштування й оптимізації використовуються такі показники, як середня й максимальна пропускні здатності. Для визначення якості мережі в цілому, не диференціюючи його за окремими сегментами або обладнаннями, використовується загальна пропускна здатність мережі, яка визначається як середня кількість інформації, переданої між усіма вузлами мережі в одиницю часу. Для визначення якості мережі так само використовують кількісний показник максимальної затримки передачі і її варіації.

Затримка передачі визначається як час знаходження пакета в будь-якому мережному обладнанні або частині мережі. Цей параметр продуктивності за змістом близький до реакції мережі, але відрізняється тим, що завжди характеризує тільки мережні етапи обробки даних, без затримок обробки комп'ютерами ЛОС.

Проведений аналіз створення розподілених систем і експлуатації ЛОС і ГОС показує, що для забезпечення їх надійності застосовуються характеристики складних систем: готовність або коефіцієнт готовності, що означає проміжок часу, протягом якого система може бути використана; вірогідність даних, тобто захист їх від викривлень; погодженість (несуперечність) та їх ідентичність.

Для опису передачі пакетів між кінцевими вузлами використовуються ймовірнісні характеристики каналу зв'язку: ймовірність доставки пакета вузлу призначення без викривлень, ймовірність втрати пакета (за кожною із причин – переповнення буфера маршрутизатора, через розбіжність контрольної суми,

через відсутність працездатного шляху до вузла призначення і т. д.), ймовірність викривлення окремого біти переданих даних.

У показник загальної надійності включається безпека – здатність системи захистити дані від несанкціонованого доступу й відмовостійкість – здатність системи сховати від користувача її окремі елементи.

При проектуванні і модернізації ЛОС ураховуються додаткові вимоги до обчислювальних мереж [15; 36; 42; 46]:

- *Розширюваність* (extensibility) – можливість порівняно легкого додавання окремих елементів мережі (користувачів, комп'ютерів, додатків, служб), нарощування довжини сегментів мережі і заміни існуючої апаратури могутнішою.

- *Масштабованість* (scalability) – можливість мережі нарощувати кількість вузлів і довжину зв'язку у дуже широких межах, при цьому зберігається показник продуктивності мережі.

- *Прозорість* (transparency) – можливість роботи з вилученими ресурсами з використанням тих же команд і процедур, що й для роботи з локальними ресурсами.

Комп'ютерні мережі споконвічно призначені для спільного доступу користувача до ресурсів комп'ютерів: файлів, принтерів і т. ін.

Проведений аналіз працездатності ЛОС (ГОС) показує, що особливу складність представляє сполучення в одній мережі традиційного комп'ютерного та мультимедійного трафіку. Для обліку складеного трафіку використовуються наступні додаткові параметри мережі:

- *Керованість* – можливість централізовано контролювати стан основних елементів мережі, виявляти й розв'язувати проблеми, що виникають при роботі мережі, виконувати аналіз продуктивності й планувати розвиток мережі.

- *Планування* – можливість прогнозування змін вимог користувачів до мережі, застосування нових додатків і мережних технологій.

Сумісність або інтегрованість – можливість включення у ЛОС (ГОС) найрізноманітнішого програмного і апаратного забезпечення (різні операційні системи, що підтримують різні стеки комунікаційних протоколів, апаратні засоби й додатка від різних виробників).

Таким чином, аналіз основних вимог, які висуваються до ЛОС і ГОС, показує, що для виконання головного завдання забезпечення користувачам потенційної можливості доступу до поділюваних ресурсів усіх комп'ютерів,

об'єднаних у мережу, необхідно виконати вимоги двох основних характеристик показника “якості обслуговування” – продуктивності і надійності.

Для оцінки надійності мережі використовуються основні характеристики складних систем: коефіцієнт готовності – проміжок часу, протягом якого система може бути використана; безпека – здатність системи захистити дані від несанкціонованого доступу й відмовостійкість – здатність системи працювати в умовах відмови деяких її елементів.

Проблема захисту комп'ютерних мереж від несанкціонованого доступу придбала особливу гостроту.

Розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значній відстані один від одного. Все це викликає збільшення числа вузлів мереж і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі й доступу до важливої інформації [15; 36; 42; 46].

Збільшення обсягів оброблюваних і переданих даних у комп'ютерних системах і мережах, насамперед, у банківських системах, у системах керування великими фінансовими і промисловими організаціями, підприємствами енергетичного сектору, транспорту нових підходів до побудови протоколів і механізмів забезпечення безпеки інформаційних систем.

Природна вимога до безпеки і вірогідності оброблюваної та переданої інформації в таких системах постає дуже гостро, оскільки відмова системи або вихід за встановлені обмеження зазначених властивостей може призвести до значних фінансових і матеріальних втрат, збитку екології, життя і здоров'я людей.

Аналіз показує [15; 20; 22 – 24; 32 – 34; 36; 41 – 42; 47; 49 – 51], що за останній час загальний обсяг оброблюваної й переданої інформації в комп'ютерних системах і мережах збільшився у декілька разів (на два – три порядки кожні п'ять – десять років) і загальні тенденції свідчать, що така динаміка збереглася.

Сучасні криптографічні засоби захисту інформації повинні забезпечувати своєчасну обробку величезних обсягів даних (десятки – сотні Мбіт/с) і задовольняти твердим вимогам з вірогідності і безпеки інформації.

Крім того, сучасний розвиток інформаційних технологій, високий рівень комп'ютеризації й інформатизації сучасного суспільства обумовили

виникнення нових загроз безпеки інформації [15; 20; 22 – 24; 32 – 34; 36; 41 – 42; 47; 49 – 51].

13.1.2. Побудова класифікацій криптографічних засобів

При розробці підходів до аналізу криптографічної захищеності інформаційної системи необхідно враховувати, яких загроз зазнає система з боку противників. Розроблені класифікації дозволяють визначити залежність атак, яких може зазнати криптосистема, від галузі її використання.

Класифікація криптографічних засобів

Існує декілька способів, відповідно до яких можуть класифікуватися криптографічні системи. Розроблена класифікація дозволяє визначити схильність криптосистеми до різних атак з боку противника, ідентифікуючи її відповідно до особливостей її реалізації. Пропонується розрізнити криптографічні засоби за критеріями, які наведені на рис. 5.2.

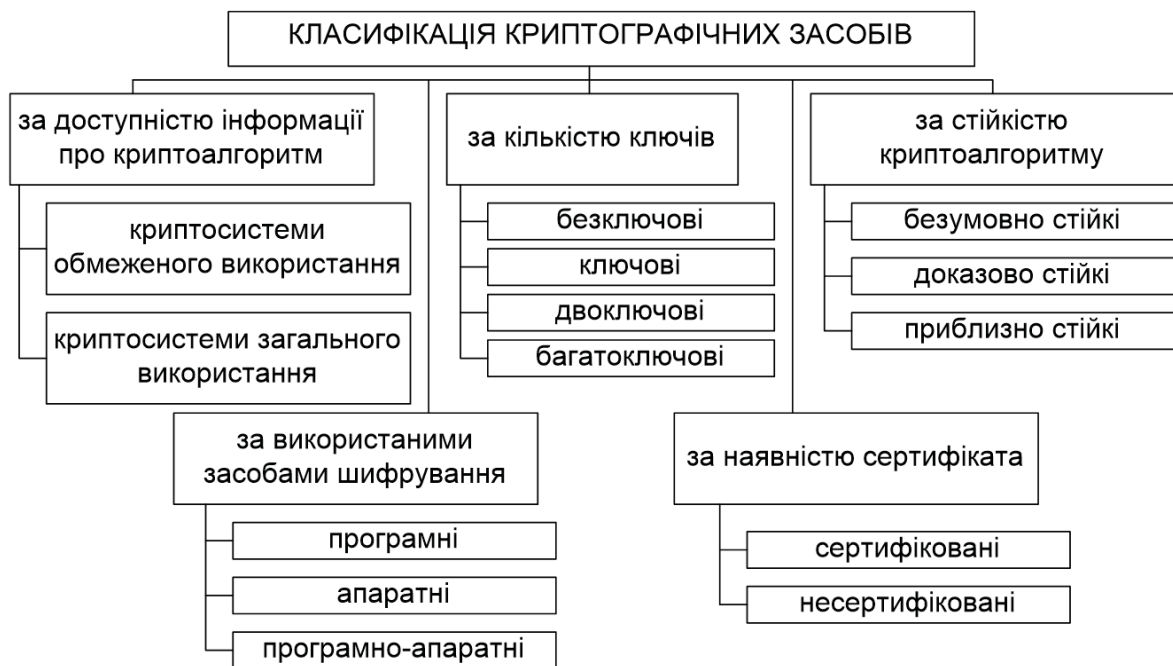


Рис. 13.2. Класифікація криптографічних засобів

Класифікація за доступністю інформації про криптоалгоритм

У роботі [53] описана наступна класифікація криптосистем:

- криптосистеми обмеженого використання;
- криптосистеми загального використання.

Криптографічна система називається *криптосистемою обмеженого використання*, якщо її стійкість ґрунтується на збереженні в секреті самого

характеру алгоритмів шифрування й розшифрування. Найпростішим прикладом такої системи можна вважати шифр Цезаря, у якому перетворення інформації зводиться до простої заміни кожного символу відкритого тексту третім, наступним за ним, символом алфавіту.

Стійкість *криптосистеми загального використання* ґрунтується не на секретності алгоритмів шифрування і розшифрування, а на секретності деякого значення, яке називається її ключем. Такий ключ повинен вироблятися конкретними користувачами таким чином, щоб навіть розроблювач криптосистеми не міг розкрити її, не маючи доступу до ключа. Зберігаючи інформацію про алгоритм у секреті, можна забезпечити деяку додаткову безпеку. Дослідження надійності таких систем завжди повинні проводитися в припущенні, що потенційному противнику відома вся інформація про криптосистему, за винятком використовуваного ключа.

Класифікація за кількістю ключів

За класифікаційною схемою, описаною в роботі [47], криптосистеми підрозділяються на 3 типи:

- *Безключові*, які не використовують ключі у процесі криптографічних перетворень.
- *Одноключові*, що використовують у своїх обчисленнях тільки секретний ключ.
- *Двоключові*, у яких на різних етапах обчислень застосовуються два види ключів: закриті (особисті) і відкриті.

Ця класифікація є неповною, тому що в ній відсутні *багатоключові* криптосистеми. До цього типу можна віднести *схеми поділу секрету*, або *(m, n)-граничні схеми*. У такій системі секретний ключ розбивається на n частин (де n – кількість учасників схеми поділу секрету) так, що за кожними m частинами можна відновити зашифровану інформацію ($m \leq n$). Отримані “частки” ключа розподіляються між усіма учасниками, після чого будь-які m учасників можуть спільно реконструювати зашифровану інформацію. В окремому випадку, коли $n = m$, для відновлення секрету необхідна присутність усіх учасників.

Класифікація за стійкістю криптоалгоритма

Здатність криптосистеми протистояти атакам криптоаналітика називається *стійкістю*. Кількісно стійкість вимірюється як складність

найкращого алгоритму, що приводить криптоаналітика до успіху із прийнятною ймовірністю. Універсальний метод прямого перебору множини всіх можливих ключів дозволяє одержати оцінку зверху для стійкості алгоритму шифрування. Відносний очікуваний *безпечний час* визначається як напівдобуток кількості відкритих ключів і часу, необхідного криптоаналітику для того, щоб випробовувати кожний ключ [27]. Залежно від мети і можливостей криптоаналітика, змінюються й стійкість. Розрізняють стійкість ключа (складність розкриття ключа найкращим відомим алгоритмом), стійкість безключового читання, імітостійкість (складність нав'язування неправильної інформації найкращим відомим алгоритмом) і ймовірність нав'язування неправильної інформації. Аналогічно можна розрізняти стійкість власне криптоалгоритму, стійкість протоколу, стійкість алгоритму генерації й поширення ключів [37].

Залежно від складності зламу алгоритми забезпечують різні ступені захисту. За основу ставиться принципова можливість одержання з перехоплення деякої інформації про відкритий текст або використаний ключ. Існують *безумовно стійкі* (або *теоретично стійкі*), *доказово стійкі* й *приблизно стійкі* криптоалгоритми.

Теоретично стійкі системи створюють шифртексти, що містять недостатню кількість інформації для однозначного визначення відповідних їм текстів (або ключів). У найкращому разі відкритий текст може бути локалізований у досить великій підмножині множини всіх відкритих текстів, і його можна лише “угадати” з мізерно малою ймовірністю. Ніякий метод криптоаналізу, включаючи повний перебір ключів, не дозволяє не тільки визначити ключ або відкритий текст, але навіть одержати деяку інформацію про них. Алгоритм безумовно стійкий, якщо відновлення відкритого тексту неможливе при будь-якому обсязі шифртексту, отриманого криптоаналітиком. Безпека безумовно стійких криптоалгоритмів заснована на доведених теоремах про неможливість розкриття ключа.

Стійкість *доказово стійких* криптоалгоритмів визначається складністю розв'язання добре відомого математичного завдання, яке намагалися розв'язати багато математиків і яке є загальновизнано складним. Як приклад можна навести системи DH (Діффі–Хелмана) і RSA (Рівеста – Шаміра–Адельмана), засновані на складностях дискретного логарифмування й розкладання цілого числа на множники відповідно. Підвищення стійкості в криптоалгоритмах досягається збільшенням розміру математичного завдання

або її заміною, що, як правило, тягне ланцюг змін в апаратурі, яка використовується для шифрування.

Приблизно стійкі криптоалгоритми засновані на складності розв'язання приватного математичного завдання, яке не зводиться до добре відомих завдань і яку намагалися розв'язати один або декілька чоловік. Прикладами можуть служити блокові шифри. Приблизно стійкі криптоалгоритми характеризуються порівняно малою вивченістю математичних завдань, на яких базується їх стійкість. Однак такі шифри мають велику гнучкість, що дозволяє при виявленні слабких місць не відмовлятися від алгоритмів, а проводити їх доробку.

Класифікація за використовуваними засобами

Розглянемо цю класифікацію в застосуванні до генераторів псевдовипадкових чисел. Для генерації ключової інформації, призначеної для використання в рамках симетричної криптосистеми, використовуються такі методи (у порядку зростання якості) [15]:

- *Програмна генерація*, що припускає обчислення чергового псевдовипадкового числа як функції поточного часу, послідовності символів, уведених користувачем, особливостей його клавіатурного почерку і т. д.
- *Програмна генерація*, заснована на моделюванні якісного псевдовипадкового генератора з рівномірним законом розподілу.
- *Апаратна генерація* з використанням якісного псевдовипадкового генератора.
- *Апаратна генерація* з використанням генераторів випадкових послідовностей, побудованих на основі фізичних генераторів шуму і якісних псевдовипадкових генераторів.

Кращий спосіб генерації множини випадкових бітів – витяг їх із природно випадкових подій реального світу [9; 19; 23]. Часто такий метод вимагає наявності спеціальної апаратури, але можна реалізувати його й на комп'ютерах. У якості випадкових величин можна також розглядати інтервали між натисканнями клавіш клавіатури. Головний недолік подібних систем – можливі закономірності в послідовності, яка генерується. Використовувані фізичні процеси можуть бути випадковими, однак використання вимірювальних інструментів може призвести до появи проблем: зсуву, відхилення або кореляції між бітами. Обійти ці недоліки можна, використовуючи не один, а декілька випадкових джерел.

Класифікація за наявністю сертифіката

Відповідно до діючого на території України законодавства, якщо організація використовує *несертифіковані* в Україні криптографічні алгоритми шифрування й електронний цифровий підпис даних, вона не може вести обмін документами з державними установами. Забезпечити юридичну значимість електронних документів при обміні ними між користувачами дозволить використання *сертифікованих* криптоалгоритмів.

Класифікація криптоаналітичних атак

Наведена на рис. 13.3 класифікація дозволяє розрізняти криптоаналітичні атаки і їх наслідки одночасно за декількома параметрами.

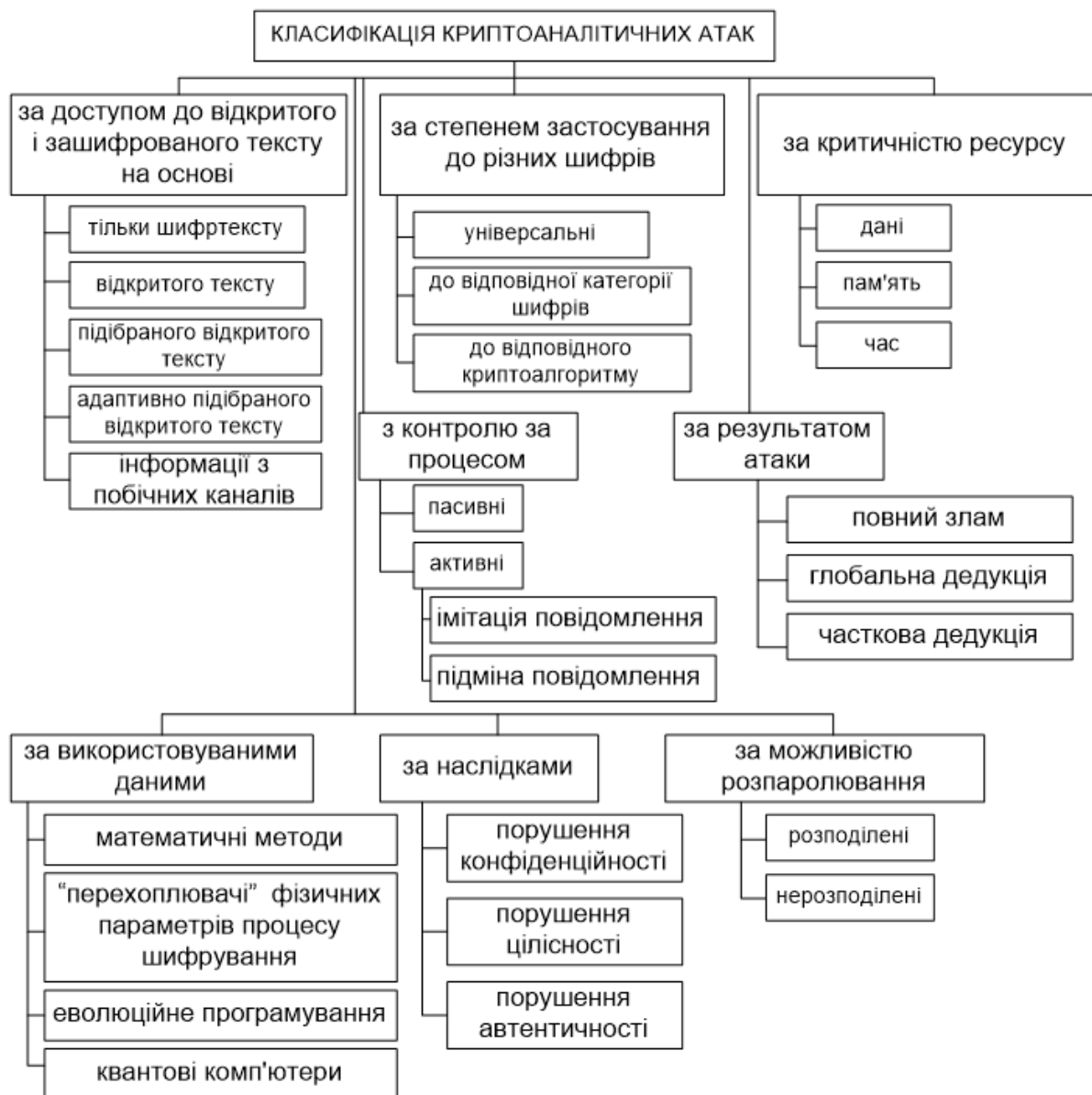


Рис.13.3. Класифікація криптографічних атак

Класифікація з доступу до відкритого й зашифрованого тексту

Перш ніж класифікувати атаки, введемо ряд позначень: відкритий текст будемо позначати буквою M , шифртекст – C (у якості M може виступати будь-яка послідовність бітів: текстовий файл і т. д.). Нехай для шифрування і розшифрування використовуються ключі k і k' відповідно (у симетричній криптографії $k = k'$); позначимо функцію шифрування E_k , розшифрування – D_k . Тоді виконуються співвідношення $E_k(M) = C$, $D_k(C) = M$. Донедавна за критерієм доступу до відкритого і шифрованого тексту виділялося чотири основні типи криптоаналітичних атак. Однак останнім часом одним із найактуальніших напрямів криптоаналізу стало здійснення атак, що використовують особливості реалізації та робочого середовища. *Атаки сторонніми або побічними каналами* – це вид криптографічних атак, що використовують інформацію, отриману зі сторонніх або побічних каналів [12]. У кожному випадку передбачається (згідно з фундаментальним допущенням Кірхгофа [17; 27; 30]), що криптоаналітик знає використовуваний алгоритм шифрування.

Атака на основі тільки шифртексту. Криптоаналітик розташовує шифртекстами $c_1, \dots, c_m$, отриманими з невідомих відкритих текстів $m_1, \dots, m_m$ різних повідомлень. Потрібно знайти хоча б один з m_i $i = 1, \dots, m$ (або відповідний ключ k_i), виходячи з достатнього числа m криптограм, або переконатися у своїй нездатності зробити це. У якості окремих випадків можливий збіг ключів або збіг відкритих текстів.

Атака на основі відкритого тексту. Криптоаналітик має у своєму розпорядженні пари $(m_1, c_1), \dots, (m_m, c_m)$ відкритих і відповідних їм зашифрованих текстів. Потрібно визначити ключ k_i для хоча б однієї з пар. В окремому випадку, коли $k_1 = \dots = k_m = k$, потрібно визначити ключ k або, переконавшись у своїй нездатності зробити це, визначити відкритий текст m_{m+1} ще однієї криптограми c_{m+1} , шифрованої на тому ж ключі.

Атака на основі підібраного відкритого тексту відрізняється від попередньої лише тим, що криптоаналітик має можливість вибору відкритих текстів $m_1, \dots, m_m$. Мета атаки та ж, що й попередньої. Подібна атака можлива, наприклад, у випадку, коли криптоаналітик має доступ до шифратора передавальної сторони.

Атака на основі адаптивно підібраного відкритого тексту. Це окремий випадок описаної вище атаки з використанням підібраного відкритого тексту. Криптоаналітик може не тільки вибирати

використовуваний текст, що шифрується, але також уточнювати свій наступний вибір на основі отриманих раніше результатів шифрування.

Атака на основі інформації з побічних каналів. Криптоаналітик має інформацію, яка може бути отримана з обладнання шифрування й не є при цьому ні відкритим текстом, ні шифртекстом.

Атаки з побічних каналів, у свою чергу, класифікуються за такими типами [12]:

- за контролем над обчислювальним процесом: *пасивні* й *активні*;
- за способом доступу до модуля: *агресивні* (invasive), *напівагресивні* (semi-invasive) і *неагресивні* (non-invasive);
- за методом, застосованим у процесі аналізу: прості – simple side channel attack (SSCA) і різницеві – differential side channel attack (DSCA);
- за видом використовуваного побічного каналу:
- атаки за часом виконання (Timing Attacks);
- атаки за енергоспоживанням (Power Analysis Attacks);
- атаки за помилками обчислень (Fault Attacks);
- атаки за електромагнітними випромінюваннями (Electro-magnetic Analysis);
- атаки за помилками у каналі зв'язку (Error Message Attacks);
- атаки за кеш-пам'яттю (Cache-based Attacks);
- акустичні атаки (Acoustic Attacks);
- атаки за світловим випромінюванням (Visible Light Attacks).

Атаки з використанням відомого або підібраного відкритого тексту зустрічаються частіше, ніж можна подумати. Необхідною вимогою до криптоалгоритму є здатність протистояти таким атакам. Це означає, що розсекречення деякої інформації, що передається каналами зв'язку в шифрованому виді, не повинне приводити до розсекречення іншої інформації, шифрованої на цьому ж ключі. Крім того, зазначена вимога враховує особливості експлуатації апаратури й допускає деякі вільності з боку оператора або осіб, що мають доступ до формування засекреченої інформації. Атаки на основі підібраних текстів вважаються найнебезпечнішими.

Класифікація з контролю над процесом шифрування

До класу *пасивних* атак [14; 20] відносять дії противника, який “пасивно вивчає” шифровані повідомлення, може їх перехопити й піддати криптоаналізу з метою одержання інформації про відкритий текст або ключ. Однак сучасні технічні засоби дозволяють потенційному противнику

“активно” втручатися в процес передачі повідомлення. Звичайно розрізняють два типи *активних* атак, які носять назви *імітації* й *підміни повідомлення*. *Атака імітації* полягає в тому, що противник “вставляє” у канал зв’язку сфабриковане ним “шифроване повідомлення”, яке насправді не передавалося від законного відправника до одержувача. При цьому противник розраховує на те, що одержувач сприйме це повідомлення як справжнє (автентичне). *Атака підміни* полягає в тому, що противник, спостерігаючи передане каналом зв’язку справжнє повідомлення від відправника, “вилучає” його й заміняє підробленим. Різні шифри можуть бути більш-менш уразливими до активних атак. Здатність самого шифру (без використання додаткових засобів) протистояти активним атакам звичайно називають *імітостійкістю шифру*. Кількісною мірою імітостійкості шифру служать ймовірності успіху імітації й підміни відповідно. Ці ймовірності визначають шанси противника на успіх при нав’язуванні одержувачу неправильного повідомлення.

Класифікація за результатом атаки

Криптоаналіз ставить своїм завданням у різних умовах одержати додаткові відомості про ключ шифрування, щоб значно зменшити діапазон ймовірних ключів. Результати криптоаналізу можуть варіюватися за ступенями практичної застосованості. Шифр вважається зламаним, якщо в системі виявлене слабе місце, яке може бути використане для більш ефективного зламу, ніж метод повного перебору ключів (“brute-force approach”). Допустимо, для дешифрування тексту методом повного перебору потрібно перебрати 2^{128} можливих ключів; тоді винахід способу, що вимагає для дешифрування 2^{110} операцій з підбору ключа, буде вважатися зламом. Такі способи можуть вимагати нереалістично великих обсягів підібраного відкритого тексту або пам’яті ЕОМ. Під *зламом* розуміється лише підтвердження наявності уразливості криптоалгоритму, що свідчить про те, що властивості надійності шифру не відповідають заявленим характеристикам. Як правило, криптоаналіз починається зі спроб зламу спрощеної модифікації алгоритму, після чого результати поширюються на повноцінну версію. Криптограф Ларс Кнудсен [93] пропонує таку класифікацію успішних наслідків криптоаналізу блокових шифрів залежно від обсягу і якості секретної інформації, яку вдалося одержати:

- *повний злам* – криптоаналітик отримує секретний ключ;

– *глобальна дедукція* – криптоаналітик розробляє функціональний еквівалент досліджуваного алгоритму, що дозволяє шифрувати й розшифровувати інформацію без знання ключа;

– *часткова дедукція* – криптоаналітику вдається розшифрувати або шифрувати деякі повідомлення;

– *інформаційна дедукція* – криптоаналітик одержує деяку інформацію про відкритий текст або ключ.

–

Класифікація за обсягом необхідних ресурсів

– Атаки можна також класифікувати за обсягом ресурсів, необхідних для їх здійснення:

– *пам'ять* – обсяг пам'яті, необхідний для реалізації атаки;

– *час* – кількість елементарних операцій, які необхідно виконати;

– *дані* – необхідний обсяг відкритих і відповідних їм зашифрованих текстів.

У деяких випадках ці параметри є взаємозалежними: наприклад, за рахунок збільшення пам'яті можна скоротити час атаки.

Класифікація за ступенем застосованості до різних шифрів

Якщо метою криптоаналітика є розкриття великої кількості шифрів (незалежно від того, чи прагне він цим завдати шкоди суспільству, попередити його про можливу небезпеку або просто одержати популярність), то для нього найкращою стратегією є розробка *універсальних методів аналізу* [12; 37]. Але це завдання є також і найбільш складним. Та обставина, що будь-яке завдання пошуку способу розкриття деякої конкретної криптосистеми можна переформулювати як привабливе математичне завдання, при розв'язанні якого вдається використовувати багато методів тієї ж теорії складності, теорії чисел і алгебри, привело до появи методів криптоаналізу, застосованих до різних класів шифрів. Нарешті, існують атаки, що використовують деяку уразливість при проектуванні або реалізації конкретного шифру. Ці атаки не можуть бути в загальному випадку перенесені на цілий клас шифрів, однак можуть ефективно застосовуватися для зламу відповідного криптоалгоритму.

Класифікація за використовуваними засобами

Та обставина, що будь-яке завдання пошуку способу розкриття деякої конкретної криптосистеми можна переформулювати як привабливе математичне завдання, при розв'язанні якого вдається використовувати

багато методів *теорії складності, теорії чисел і алгебри*, привело до розкриття багатьох криптосистем. Майже всі здійснені на практиці вдалі атаки на криптосистеми використовують слабкості в реалізації й розміщенні механізмів криптоалгоритму. Такі атаки засновані на кореляції між значеннями *фізичних параметрів, вимірюваних у різні моменти під час обчислень* (споживання енергії, час обчислень, електромагнітне випромінювання і т. п.), і внутрішнім станом обчислювального обладнання, що мають відношення до секретного ключа. На практиці атаки побічними каналами на багато порядків більш ефективні, ніж традиційні атаки, засновані тільки на математичному аналізі. При цьому атаки побічними каналами використовують особливості реалізації (тому їх іноді також називають атаками на реалізацію – *implementation attacks*) для витягання секретних параметрів, задіяних в обчисленнях. Такий підхід менш узагальнений, оскільки прив'язаний до конкретної реалізації, але найчастіше могутніший, ніж класичний криптоаналіз. На даний момент методи, засновані на використанні нових інформаційних технологій (еволюційного програмування і квантових комп'ютерів), у криптоаналізі не привели до серйозних проривів у зламі шифрів і мають скоріше академічний інтерес, ніж практичний.

Криптосистему можна розглядати як “чорний ящик”, тобто обладнання або програму, про внутрішню структуру якої нічого не відомо, але, подаючи сигнали команди або дані на вхід, можна одержати реакцію на виході. Завдання криптоаналізу – ідентифікація цієї системи, тобто визначення її структури на основі сигналів, що надходять на її вхід і одержуються на виході. Одним з інструментів розв'язання цього завдання можуть бути нейронні мережі [13]. Генетичні алгоритми успішно застосовуються в криптоаналіз переставних і підставних шифрів [42; 47].

Класифікація за наслідками атаки

Можливі наслідки реалізації атаки розглянемо з погляду порушення властивостей інформації – конфіденційності, цілісності й автентичності (доступності). Можна виділити три стратегії дій, які може почати порушник у випадку успішної реалізації атаки.

Перехоплення інформації, переданої каналами зв'язку.

Модифікація інформації, переданої каналами зв'язку (підміна, неправильні повідомлення, блокування передачі і т. д.).

Робота від чужого імені (обхід засобів автентичності учасників інформаційної взаємодії каналами зв'язку).

Класифікація за можливістю розпаралелювання

Розпаралелюванню піддаються не всі алгоритми криптоаналізу, однак воно дозволяє значно прискорити знаходження ключа. Таким чином, при оцінці ефективності методу криптоаналізу необхідно враховувати не тільки його часову і ємнісну складність, але й можливість розпаралелювання на багатопроцесорній системі. Так, алгоритм Полларда має складність $O(\sqrt{n})$, однак *не піддається розпаралелюванню*. У той же час метод повного перебору, який на однопроцесорній машині уступає за ефективністю методу Полларда, становить простий приклад методу криптоаналізу, що *допускає розпаралелювання*.

Відомо два напрямки в організації паралельного обчислення ключа [17; 30; 31]. По-перше, побудова конвеєра. Нехай алгоритм співвідношення $E_k(M) = C$ представимо у вигляді детермінованого ланцюжка найпростіших дій (операцій): $O_1, O_2, \dots, O_N$. Візьмемо N процесорів $A_1, A_2, \dots, A_N$, задамо їх порядок і доведемо, що i -й процесор виконує три однакові за часом операції:

- 1) приймання даних від $(i - 1)$ -го процесора;
- 2) виконання операції O_i ;
- 3) передача даних наступному $(i + 1)$ -му процесору.

Тоді конвеєр з N послідовно з'єднаних процесорів, що паралельно й синхронно працюють зі швидкістю $\frac{v}{3}$, де v – швидкість виконання однієї операції процесором.

Другий напрямок розпаралелювання полягає в тому, що множина K розбивається на непересічні підмножини $K_1, K_2, \dots, K_Q$. Система з Q машин перебирає ключі так, що i -а машина здійснює перебір ключів з множини $K_i, i = \overline{1, Q}$. Система припиняє роботу, якщо одна з машин знайшла ключ. Найбільшою складністю у викладеному підході є організація розподілу ключової множини. Однак якщо організувати пошук ключа таким чином, що при кожному черговому випробуванні кожний з N процесорів стартує з випадкової точки, то час випробування збільшиться, але схема значно спроститься. Як показано в роботі [6], середня кількість кроків випробування N процесорами (машинами) ключів з множини K у цьому випадку становить $\frac{|K|}{N}$. Реалізація такого паралелізму припускає різні розв'язання. Найбільш

очевидне розв'язання – створення комп'ютерного вірусу для поширення програми-зломщика в глобальній мережі. Вірус повинен використовувати періоди простою комп'ютера (за даними досліджень, комп'ютер простоює 70 –

90 % часу) для здійснення перебору за множиною ключів. Рано або пізно один із заражених комп'ютерів виявить шуканий ключ (необхідно передбачити механізм сповіщення противника); зі зростанням продуктивності комп'ютерів і швидкості поширення вірусів загроза успішного результату такої атаки зростає.

Класифікація зломищиків криптосистем

При оцінці стійкості криптосистеми необхідно брати до уваги можливість потенційного противника, який може здійснити атаки на систему. Інакше кажучи, необхідно попередньо відтворити збірний образ (модель) порушника. Така модель повинна вказувати [10]:

- категорії осіб, у числі яких може виявитися порушник;
- припущення про кваліфікацію порушника і його технічну оснащеність;
- можливі цілі порушника й очікуваний характер його дій.

За основу для розробки класифікаційної схеми була прийнята модель порушника, запропонована в [35]. Запропонована в даній роботі класифікація дозволяє при побудові моделі зломщика криптосистеми враховувати різні параметри й, тим самим, встановити залежність можливих сценаріїв атак від характеристик противника, з боку яких система піддається нападам. На рис. 13.4 наведена класифікація противника.

Класифікація за технічною оснащеністю

На сьогоднішній день великій компанії з великими обчислювальними мережами під силу методом перебору розкрити ключ довжиною 64 – 80 бітів. Підтвердженням цьому є розкриття RC5-64 (блокового шифру компанії RSA, що використовує 64-бітний ключ, що стартував в 1997 році на сайті www.distributed.net (проект “розподіленого зламу”) [33], у якому на добровільній основі взяли участь більш 300 тисяч користувачів глобальної мережі, був успішно завершений за п'ять років (1 757 днів) – за цей час було перебрано 85 % всієї множини ключів.

Крім того, для розв'язання завдань криптоаналізу можна використовувати суперкомп'ютери. У [50] наведений список організацій, що володіють найпотужнішими суперкомп'ютерами, й здатних займатися перехопленням і дешифруванням інформації, та описана залежність зростання потужності суперкомп'ютерів від часу, виходячи з якої можна визначити можливу стійкість криптоалгоритмів.



Рис. 13.4. Класифікація порушника криптосистем

Класифікація за кінцевою метою

В основі дій хакерів звичайно лежить корислива мотивація, рідше – бажання прославитися, завдати моральної шкоди законному власнику шифрованої інформації або інші причини. Мета криптоаналітика полягає у створенні нових і підвищенні ефективності існуючих методів аналізу стійкості криптографічних засобів. Кожний новий метод криптоаналізу приводить до перегляду безпеки шифрів, до яких він застосовний.

Класифікація за доступом до засобів, що шифрують

Порушником може бути не тільки стороння особа, але й законний користувач системи, а також особа із числа обслуговуючого персоналу [10]. Якщо в ролі зломщиків виступають ненадійні співробітники компанії, то можливостей для здійснення атак з'являється набагато більше, ніж у будь-яких інших зломщиків.

Класифікація за рівнем підготовки

Кваліфікація зломщика визначається наявністю релевантних знань, умінь і навичок. Можна виділити чотири основні області, освоєння яких може бути корисним порушнику для здійснення атаки на криптосистему:

- *взаємодія з комп'ютером на рівні користувача* – для здійснення атак з використанням доступних інструментальних засобів;

– *математичний апарат* – для створення нових методів криптоаналізу й підвищення ефективності існуючих методів;

– *програмування* – для розробки інструментальних засобів, що реалізують алгоритми криптоаналізу; створення вірусів для розпаралелювання пошуків ключа й т. п.;

– *електротехніка та фізика* – для реалізації криптоатак побічними каналами з використанням інформації, яку можна витягти з обладнання, що шифрує. Наприклад, зломщик може відслідковувати енергію, споживану смарт-картою, коли вона виконує операції із закритим ключем, такі, як розшифрування або генерація підпису. Порушник може також заміряти час, затрачений на виконання криптографічної операції або аналізувати поведінку криптографічного обладнання при виникненні певних помилок [83];

– *соціальна інженерія* – потужна зброя зломщика, що дозволяє обійти захист найстійкіших криптосистем, скориставшись довірливістю користувачів.

Градація противників за їх кваліфікацією може бути різною. Наприклад, в [19] виділено три класи противника:

- висококваліфікований зловмисник-професіонал;
- кваліфікований зловмисник-непрофесіонал;
- некваліфікований зловмисник-непрофесіонал.

Класифікація за первинною інформацією про засіб шифрування

Порушнику може бути відома інформація (у тому числі секретна) про принципи функціонування криптосистеми. Так, однією із причин ненадійності криптосистем є використання слабких ключів. Слабкий ключ – це ключ, що не забезпечує достатнього рівня захисту або, той що використовує в шифруванні закономірності, які можуть бути зламані. Це означає що, якщо для генерації ключів використовується криптографічний слабкий алгоритм, то незалежно від шифру, який використовується, вся система буде нестійкою [47]. *Генератори випадкових чисел* – те місце, у якому часто ламаються криптографічні системи. Знаючи принцип витягу випадкових чисел, противник може значно скоротити область перебору можливих ключів системи.

Особливої уваги заслуговує технологія, описана в роботі [13] за назвою “*клеттографія*”. Розроблювач може випадково або навмисно вмонтувати у криптосистему лазівки, що дозволяють одержувати доступ до зашифрованої

інформації без знання секретного ключа. Через “чорний хід” інформована людина може легко подолати захист. Якщо механізм дії шифру тримається в секреті, ймовірність наявності подібної “лазівки” підвищується.

Класифікація за можливістю кооперації

Останнім часом у зв’язку з розвитком мереж (зокрема, Інтернету) стало можливо ефективно використовувати метод “грубої сили” (перебору) шляхом розпаралелювання операцій. Нерідко професійні хакери поєднуються у злочинні угруповання, що прагнуть до наживи й виконуючі розкрадають конфіденційну інформацію із замовлень конкуруючих фірм і навіть іноземних спецслужб [10]. Альтернативний варіант – створення вірусу, непомітно для користувача, що встановлює на підключений до мережі комп’ютер програму, здатну здійснювати дешифрування повідомлення шляхом перебору ключів. Сценарій такої колективної атаки простий і описаний, наприклад, у [35; 37]. Після запуску програма підключається до сервера, одержує від нього набір ключів для перебору й після закінчення роботи повертає результат. Програма може працювати у фоновому режимі, у якості скринсейвера або активуватися ночами. Такий підхід застосуємо не тільки для зламу шифрів, але і для підбору двох текстів, що мають однакове значення хеш-функції, обчисленої зазначеним алгоритмом. На рис. 13.5 наведений приклад класифікації загроз інформації для кіберфізичної моделі на прикладі об’єктів критичної інфраструктури банківського сектору.

Таким чином, оцінка ефективності криптографічних засобів захисту інформації становить складне науково-технічне завдання.

При виборі криптосистеми необхідно проводити аналіз загроз безпеки в конкретній комп’ютерній системі, що передбачає оцінку стійкості до досить різноманітних типів криптоаналітичних нападів.

Модель загроз можна розглядати як композицію моделі противника, моделі атак і моделі криптосистеми. Ці моделі можуть бути побудовані на основі наведених класифікацій.

13.1.3. Побудова моделі порушника безпеки в КМіС

Спроба одержати несанкціонований доступ до комп’ютерних мереж з метою ознайомитися з ними, залишити записку, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як комп’ютерне піратство. Як соціальне явище, подібні дії прослідковуються в останні 10

років, але при цьому спостерігається тенденція до їх стрімкого зростання по мірі збільшення кількості побутових комп'ютерів.

Зростання кількості комп'ютерних порушень очікується в тих країнах, де вони широко рекламуються у фільмах і книгах, а діти у процесі ігор рано починають знайомитися з комп'ютерами. Разом з тим зростає кількість серйозних навмисних злочинів [53].

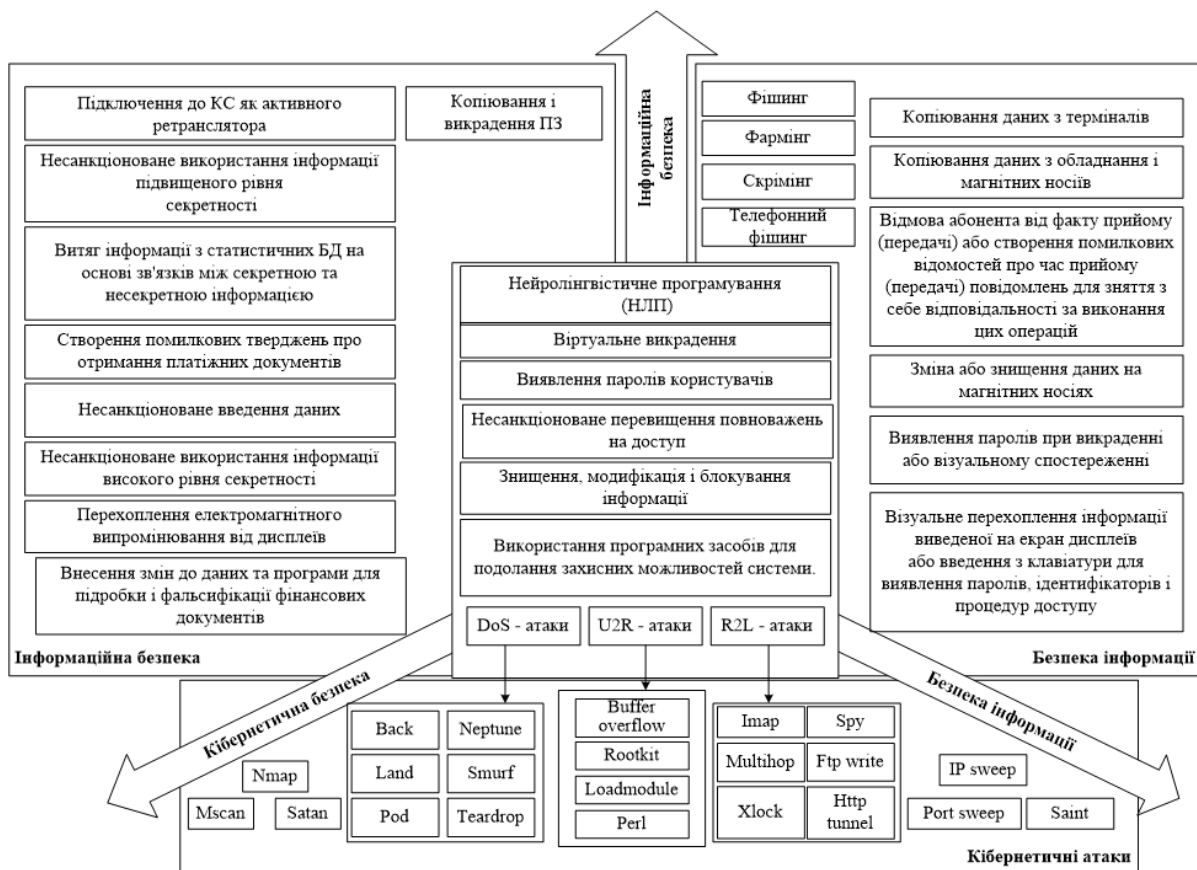


Рис. 13.5. Класифікація загроз синергетичної моделі

Однак комп'ютерні злочинці не цікавляться, наскільки добре здійснюється в цілому контроль у комп'ютерній системі; вони шукають єдину лазівку, яка приведе їх до бажаної мети. Для одержання інформації вони проявляють винахідливість, використовуючи психологічні фактори, детальне планування та активні дії. Необхідно розділити два визначення: хакер (hacker) і кракер (cracker). Основна відмінність полягає в постановці мети зламу комп'ютерних систем: перші ставлять дослідницькі завдання з оцінки і знаходження уразливостей з метою наступного підвищення надійності комп'ютерної системи. Кракери ж втручаються в систему з

метою руйнування, крадіжки, псування, модифікації інформації і роблять правопорушення з корисливими намірами швидкого збагачення.

Для запобігання можливих загроз необхідно не тільки забезпечити захист операційних систем, програмного забезпечення і контроль доступу, але й виявити категорії порушників і ті методи, які вони використовують.

Залежно від мотивів, цілей і методів дії порушників безпеки інформації можна розділити на чотири категорії:

- шукачі пригод;
- ідейні хакери;
- хакери-професіонали;
- ненадійні (неблагополучні) співробітники.

Шукач пригод, як правило, це студент, у якого рідко є продуманий план атаки. Він вибирає мету випадковим чином і звичайно відступає, зіштовхнувшись із труднощами. Знайшовши діру в системі безпеки, він намагається зібрати закриту інформацію, але практично ніколи не намагається її таємно змінити. Своїми перемогами такий шукач пригод ділиться тільки зі своїми близькими друзями-колегами.

Ідейний хакер – це той же шукач пригод, але більш митецький. Він уже вибирає собі конкретні цілі (хости та ресурси) на підставі своїх переконань. Його улюбленим видом атаки є зміна інформаційного наповнення Web-сервера або, у більш рідких випадках, блокування роботи ресурсу, що атакуються. Порівняно з шукачем пригод, ідейний хакер розповідає про успішні атаки набагато більш широкій аудиторії, звичайно розміщаючи інформацію на хакерському Web-вузлі або в конференціях Usenet.

Хакер-професіонал має чіткий план дій і націлюється на конкретні ресурси. Його атаки добре продумані й звичайно здійснюються в кілька етапів. Спочатку він збирає попередню інформацію (тип операційної системи (ОС), надавані сервіси й застосовує заходи захисту). Потім він становить план атаки з урахуванням зібраних даних і підбирає (або навіть розробляє) відповідні інструменти. Провівши атаку, він одержує закриту інформацію, і нарешті, знищує всі сліди своїх дій. Такий атакуючий професіонал звичайно добре фінансується й може працювати самому або у складі команди професіоналів.

Ненадійний (неблагополучний) співробітник своїми діями може доставити стільки ж проблем (буває й більше), скільки промисловий шпигун, до того ж його присутність, звичайно, складніше виявити. Крім того, йому

доводиться долати не зовнішній захист мережі, а тільки, як правило, менш твердий внутрішній захист. Він не так витончений у способах атаки, як промисловий шпигун, і тому частіше допускає помилки й тим самим може видати свою присутність. Однак у цьому випадку небезпека його несанкціонованого доступу до корпоративних даних багато вище, ніж будь-якого іншого зловмисника. Перераховані категорії порушників безпеки інформації можна згрупувати за їх кваліфікацією: *початківець* (шукач пригод), *фахівець* (ідейний хакер, ненадійний співробітник), *професіонал* (хакер-професіонал).

Порушник безпеки інформації, як правило, будучи фахівцем визначеної кваліфікації, намагається довідатися про комп'ютерні системи й мережі і, зокрема, про засоби їх захисту. Тому модель порушника визначає [28]:

- категорії осіб, у числі яких може виявитися порушник;
- можливі цілі порушника і їх градації за ступенями важливості й небезпеки;
- припущення про його кваліфікації;
- оцінка його технічної озброєності;
- обмеження й припущення про характер його дій.

На рис. 13.6 наведена узагальнена модель порушника безпеки інформації.

Діапазон спонукальних мотивів одержання доступу до системи досить широкий: від бажання випробувати емоційний підйом при грі з комп'ютером до відчуття влади над ненависним менеджером. Займаються цим не тільки новачки, що бажають побавитися, але й професійні програмісти. Паролі вони добувають або в результаті підбору або шляхом обміну з іншими хакерами.

Частина з них, однак, починає не тільки переглядати файли, але й проявляти інтерес саме до їх змісту, а це вже являє серйозну загрозу, оскільки в цьому випадку важко відрізнити невинне баловство від злочинних дій.

Донедавна викликали занепокоєння випадки, коли незадоволені керівником службовці, зловживаючи своїм положенням, псували системи, допускаючи до них сторонніх або залишаючи системи без догляду в робочому стані. Спонукальними мотивами таких дій є:

- реакція на догану або зауваження з боку керівника;

- невдоволення тим, що фірма не оплатила понаднормові години роботи (хоча найчастіше понаднормова робота виникає через неефективне використання робочого часу);
- злий намір у якості реваншу з метою послабити фірму як конкурента якої-небудь фірми.



Рис. 13.6. Модель порушника безпеки інформації

Незадоволений керівником службовець створює одну із найбільших загроз обчислювальним системам колективного користування.

Професійні хакери – це комп’ютерні фанати, що прекрасно знають обчислювальну техніку і системи зв’язку. Вони затратили масу часу на обмірковування способів проникнення в системи й ще більш, експериментуючи із самими системами. Для входження в систему професіонали найчастіше використовують деяку систематику й експерименти, а не розраховують на удачу або здогад. Їх мета – виявити й подолати захист, вивчити можливості обчислювальної установки й потім вийти, ствердившись у можливості досягнення своєї мети.

Завдяки високій кваліфікації ці люди розуміють, що ступінь ризику малий, тому що відсутні мотиви руйнування або розкрадання. До категорії хакерів-професіоналів звичайно відносять таких осіб:

- які відносяться до злочинних групувань, що переслідують політичні цілі;

- прагнучих одержати інформацію з метою промислового шпигунства;
- хакерів або угруповання хакерів, що прагнуть до наживи.

Для здійснення несанкціонованого доступу в інформаційну систему потрібно, як правило, провести два підготовчі етапи:

- зібрати відомості про систему;
- виконати пробні спроби входження в систему.

Збір відомостей. Залежно від особистості зломщика і його похилостей можливі різні напрямки збору відомостей:

- підбір співучасників;
 - аналіз періодичних видань, відомчих бюлетенів і документації;
 - перехоплення повідомлень електронної пошти;
 - підслуховування розмов, телексів, телефонів;
 - перехоплення інформації й електромагнітного випромінювання;
- організація крадіжок;
- вимагання й хабар.

Багато власників систем часто не уявляють, яку підготовчу роботу повинен провести порушник, щоб проникнути в ту або іншу комп'ютерну систему. Тому вони самовпевнено вважають, що єдине, що необхідно зробити, – це захистити файл, указавши йому пароль, і забувають, що будь-яка інформація про ті або інші слабкі місця системи може допомогти зломщику знайти лазівку й обійти пароль, одержавши доступ до файлу. Таким чином, інформація стає легкодоступною, якщо зломщик знає, де й що дивитися.

Підбір співучасників. Підбір співучасників заснований на підслуховуванні розмов у барах, фойє готелів, ресторанах, таксі, підключенні до телефонів і телексам, вивченні змісту загублених портфелів і документів. Багато корисної інформації можна витягти, якщо трапляється можливість підсісти до групи програмістів. Цей спосіб часто використовують репортери й професійні агенти.

Витяг інформації з періодичних видань. Зломщики можуть почерпнути багато корисної інформації з газет і інших періодичних видань.

Перехоплення повідомлень електронної пошти. Звичайно для підключення до електронної пошти використовується побутовий комп'ютер з модемом для зв'язку з державною телефонною мережею [28].

Телефонний канал доступу в таку систему звичайно вільний, хоча останнім часом системні оператори вимагають установки обладнань реєстрації користувачів електронної пошти. Аж до недавнього часу багато довідкових систем були оснащені блоками, через які зломщики могли витягати великі обсяги даних, а також ідентифікатори й паролі користувачів. Зараз немає нічого незвичайного в тому, що блоки, встановлені кракерами, можуть бути зашифровані й тільки окремі члени злочинних угруповань можуть зчитувати з них інформацію.

Зав'язування знайомств. З метою одержання інформації про обчислювальну систему або отримання службових паролів зломщики можуть використовувати різноманітні способи. Наприклад, знайомлячись, вони представляються менеджерами; використовують запитальники, роздаючи їх у фойє фірми й детально розпитуючи співробітників про комп'ютерну систему; дзвонять системному адміністратору в обідній час із проханням нагадати нібито забутий пароль; прогулюються в будинку, спостерігаючи за доступом до системи; встановлюють контакти з незайнятими в цей момент службовцями охорони, яким відвідувачі при вході в будинок фірми повинні пред'являти ідентифікаційний код або пароль.

Більш зловмисним, але, можливо, і більш успішним є метод “полювання за розумами”, коли на фірму приходить людина, яка бажає працювати системним програмістом або інженером зв'язку, і просить дати йому консультацію. Дивно, як багато інформації може передати службовець, який не має перспективи росту, але, вважає себе гідним більш важливої й високооплачуваної посади; він може розкрити коди користувачів, паролі, указати слабкі місця в мережах зв'язку і т. д.

Аналіз роздруківок. Деякі зломщики одержали доступ, до ЕОМ просто вивчаючи роздруківки, і це один з найбільш ефективних і найменш ризикованих шляхів одержання конфіденційної інформації. Численні фірми втрачають інформацію зі своїх комп'ютерних систем, по-перше, помилково думаючи, що вона не містить конфіденційної інформації, і, по-друге, помилково вважаючи, що всі чорнові роздруківки сумлінно знищуються. Саме таким способом зломщики змогли одержати досить повну картину організації комп'ютерної системи, використовуючи викинуті роздруківки й незатребувані протоколи роботи системи, які співробітникам обчислювального центру представлялися невинними папірцями.

Перехоплення повідомлень в каналах зв'язку. На сьогодні кількість фірм, оснащених обчислювальною технікою, постійно зростає, тому

перехоплення повідомлень стало досить реальною загрозою й для комерційного світу. Спектр можливих перехоплень досить широкий – перехоплення усних повідомлень із використанням радіопередавачів, мікрофонів і мікрохвильових обладнань; підслуховування повідомлень, переданих з телефону, телексу й іншими каналами передачі даних; контроль електромагнітного випромінювання від ПК; перехоплення супутникових або мікрохвильових передач.

Установкою радіопередавачів, мікрофонів і мікрохвильових обладнань або прослуховуванням ліній зв'язку звичайно займаються професійні зломщики, а також аматори й фахівці зі зв'язку. Останнім часом кількість випадків установки таких обладнань зростає. Улюбленими точками безконтрольного доступу також є телефонні лінії.

Передача даних з комутацією пакетів або з використанням широкосмугових ліній зв'язку зі швидкостями в тисячу й мільйони бод викликає інтерес у зломщиків і може бути перехоплена, щоб викрасти передані повідомлення, модифікувати їх зміст, затримати або вилучити.

Формально удосконалену модель зловмисника визначимо на прикладі банківського сектору:

$$G_{IA}^{ABS} = \{aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS}\} \forall i \in n, \forall j \in m,$$

де $aid_i \in \{aid\}$ – ідентифікатор зловмисника (категорія зловмисника);

$pur_i \in \{pur_i\}$ – мета зловмисника; T_{IA} – час успішної реалізації загрози;

$S_{\max_i}$ – ймовірний збиток системи; $MS_i^{ABS} = \{ms_i\}_{i=1}^{N_{MS^{ABS}}}$ – рекомендації

щодо виявлення, реагування технічні засоби захисту інформації (ТЗЗІ),

$N_{MS^{ABS}}$ – кількість рекомендацій відомих АБС; n – кількість загроз; m – кількість активів банківських інформаційних ресурсів(БІР).

Множина джерел загроз включає джерела чотирьох видів:

$$DF^{ABS} = \{V^{NS}, V^{AS}, TS, PI, NI\},$$

де DF^{ABS} – множина джерел загроз безпеці автоматизованої банківської системі (АБС), в якій V^{NS} – клас природних джерел загроз;

$V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKB}\}$ – клас антропогенних загроз, де V^{ASIB} – множина загроз ІБ; V^{ASBI} – множина загроз БІ; V^{ASKB} – множина загроз кібербезпеки (КБ);

TS – технічні засоби і системи; PI – навмисні зловмисники; NI – ненавмисні зловмисники.

Сценарієм реалізації загроз називається один або кілька пов'язаних переходів компонентів АБС в деструктивні стани в результаті впливів джерел загроз. Один або кілька сценаріїв реалізації загроз можуть бути представлені орієнтованим графом $G(V, H)$, в якому: початковою вершиною (v_0) є множина, один з видів або конкретне джерело загроз; проміжними і кінцевими вершинами (v_n) є деструктивні стани компонентів АБС; дугами (h_{ij}) з'єднуються дві вершини, одна з яких є причиною (v_i), а друга – наслідком і результатом переходу (v_j).

Для оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів визначимо набори зважених метрик, які набувають значення в інтервалі $[0; 1]$. Кожна метрика характеризує ступінь відповідності певної ознаки зловмисника або захисний засіб заданому цільовому значенню.

Для оцінки ступеня небезпеки зловмисника будемо вважати, що він має такі характеристики (*Capabilities*) по відношенню до АБС: $C = \{\text{мотивація (motivation, } M), \text{ оснащеність/наявне обладнання (equipment, } O), \text{ технічна компетентність (technical competence, } K), \text{ володіння інформацією про АБС і ТЗЗІ (possession of information on the automated banking system and technical means of information protection, } I), \text{ доступні до реалізації загрози права доступу (access rights, } D), \text{ час до моменту реагування ТЗЗІ на атаку (response time to attack, } T)\}$. Таким чином, маємо таку множину характеристик зловмисника: $C = \{M, O, K, I, D, T\}$. Для опису множини характеристик використаємо індекс h : C_h , де $(\{h\}_1^C)$.

Нехай j – послуги безпеки БІР. Основними послугами безпеки БІР є C – конфіденційність; I – цілісність; A – доступність; Au – автентичність. Тоді класифікатор за чотирьох послугами безпеки описується виразом вигляду $j = \{C, I, A, Au\}$.

Позначимо через i поточний номер зловмисника $(\{i\}_1^L)$, через k – поточний номер експерта, який виконував оцінку $(\{k\}_1^K)$. Відповідно, ми будемо мати L зловмисників та K експертів. Позначимо також через w_{kih}^j – експертну оцінку k -го експерта для h -ї характеристики i -го зловмисника для j -ї послуги безпеки.

Тоді середнє значення оцінок усіх експертів за усією сукупністю характеристик усіх зловмисників для j -ї послуги безпеки буде мати вигляд:

$$w^j = \frac{1}{KLC} \sum_{k=1}^K \sum_{i=1}^L \sum_{h=1}^C \alpha_{kih}^j \times w_{kih}^j,$$

де α_{kih}^j – ваговий коефіцієнт h -ї метрики i -го зловмисника для j -ї послуги. Вагові коефіцієнти підкоряються умові нормування, тобто $\sum_{k=1}^K \sum_{i=1}^L \sum_{h=1}^C = 1$.

Аналогічним чином можна описати ступінь захищеності ТЗЗІ АБС. Для цього використаємо множину характеристик $B = \{\text{cryptographic resistance, стійкість ТЗЗІ } (C_r), \text{ обсяг ключових даних (Key data amount, } S_c), \text{ складність виконання прямого і оберненого криптографічного перетворення (шифрування/розшифрування БР) (encryption/decryption of data, } O_E)\}$. Таким чином, маємо таку множину характеристик ТЗЗІ: $B = \{C_r, S_c, O_E\}$. Для опису множини характеристик використаємо індекс g : B_g , де $(\{g\}_1^B)$. Позначимо через w_{kg}^j – значення оцінки g -ї характеристики ТЗЗІ k -м експертом для j -ї послуги безпеки у випадку, коли ступінь захищеності системи та деструктивні дії зловмисників незалежні.

Тоді середнє значення оцінок усіх експертів ступені реалізації захисних заходів для j -ї послуги безпеки буде мати вигляд:

$$\psi^j = \frac{1}{KB} \sum_{k=1}^K \sum_{g=1}^B (\beta_{kg}^j \times w_{kg}^j),$$

де β_{kg}^j – ваговий коефіцієнт g -ї метрики j -ї послуги безпеки для k -го експерта.

Нормування вагових коефіцієнтів звичайне: $\sum_{k=1}^K \sum_{g=1}^B \beta_{kg}^j = 1$.

Для кореляції між ступенем небезпеки зловмисника та характеристиками захисту системи, тобто між множинами C та B . використаємо матрицю M розміром $[C \times B]$, яку іноді називають матрицею парних порівнянь. Якщо g -а захисна характеристика B_g повністю блокує h -ту властивість зловмисника (або загрозу, яка реалізується цим зловмисником), то $M_{hg} = 1$. в іншому випадку $M_{hg} = 0$. Можливі також проміжні значення, коли загроза/характеристика зловмисника закривається не повністю. Таким чином, M_{hg} – матриця коефіцієнтів, які пов'язують між собою загрози/характеристики зловмисника із захисними заходами системи безпеки.

Тоді нові значення оцінок захисних заходів з використанням матриці M можна записати:

$$(w_{kg}^j)_{cor} = M_{hg} \times w_{kg}^j.$$

Тоді

$$\psi^j = \frac{1}{KB} \sum_{k=1}^K \sum_{g=1}^B (\beta_{kg}^j \times (w_{kg}^j)_{cor}).$$

Формування експертної групи (кількість експертів) обчислимо за формулою:

$$K \geq 0,5(0,33 / \beta + 5),$$

де β – помилка результату експертного аналізу або допустима ймовірність помилки.

Оцінюється індекс узгодженості оцінок експерта за виразом:

$$C_E = \frac{\lambda_{k_{\max}} - m}{m - 1},$$

де $\lambda_{k_{\max}}$ – максимальна власна кількість матриці парних порівнянь k -го експерта;

m – розмірність матриці парних порівнянь.

Оцінки експерта вважаються узгодженими, якщо відношення узгодженості $CR = C_E/CIS$, де CIS – середнє значення індексу узгодженості, який визначається в діапазонах (табл. 13.1).

Таблиця 13.1

Значення CIS і CR від m

m	3	4	5	6	7	8	9	10	11	12
CIS	0,58	0,90	1,12	1,24	1,32	1,41	1,45	1,49	1,51	1,48
CR	[0;0,05]	[0;0,08]	[0, 0,1]							

Неприйнятні оцінки повинні бути скоректовані експертом, в іншому випадку їх не слід враховувати при розрахунку результуючого вектора пріоритетів. Узгодженість думок групи експертів визначається за правилом трьох сігм. Неузгоджені оцінки не враховуються при розрахунку

результуючого вектора пріоритетів $\bar{B} = (\bar{b}_1, \bar{b}_2, \dots, \bar{b}_m)^T$, $\bar{b}_i = \sqrt[K]{\prod_{k=1}^K b_{ik}}$,

де $\bar{b}_i$ – результуючий пріоритет елементу x_i ;

K – кількість експертів.

Думки експертів вважаються узгодженими, якщо все пріоритети b_{ik} лежать в інтервалі $(\bar{b}_i - 3\sigma_{gi}; \bar{b}_i + 3\sigma_{gi})$, де σ_{gi} – геометричне стандартне відхилення вагового коефіцієнта b_{ik} , яке визначається за виразом:

$$\sigma_{gi} = e^{\left(\sqrt{\frac{1}{K} \sum_{k=1}^K \ln \frac{b_{ik}}{\bar{b}_i}} \right)^2}$$

Довірчий інтервал δ_i визначається за формулою:

$$\delta_i = t_{cm} \times \sigma_{gi} / \sqrt{K},$$

де $t_{cm}=0,95$ – критерій Стюдента.

У ході аналізу документів з моделювання загроз, оцінки ризиків та теорії надійності визначені такі деструктивні стани елементів АБС (множина $\{VH\}$):

а) *інформаційний актив*:

- недоступний (порушена доступність), $I_A^{[D]}$;
- скомпрометований (порушена конфіденційність), $I_A^{[K]}$;
- змінений (порушена цілісність), $I_A^{[C]}$;
- порушена мітка безпеки (цифровий підпис) (порушена автентичність), $I_A^{[A]}$;

б) *програмне забезпечення*:

- недоступне (стався збій), $SW^{[B]}$;
- зламане (відбувся несанкціонований доступ (НСД) зловмисником або підвищені привілеї користувача), $SW^{[I]}$;
- порушення доступності, $SW^{[U]}$;
- змінене (несанкціоновано змінений код і / або конфігурація), $SW^{[M]}$;

в) *технічний засіб*:

- недоступний (стався тимчасовий збій), $HW^{[B]}$;
- порушення доступності, $HW^{[U]}$;
- непрацездатний (відбулася відмова, що вимагає ремонту або заміни), $HW^{[D]}$;
- загублено (відбулася втрата або крадіжка у законного власника), $HW^{[L]}$;

– зламано (відбувся несанкціонований доступ (НСД) зловмисником або було перевищено повноваження), $HW^{[I]}$;

г) лінія зв'язку:

– недоступна (відбувся збій або відмова), $CL^{[D]}$;

– порушення доступності, $CL^{[U]}$;

– зламано (відбувся НСД зловмисником), $CL^{[I]}$.

13.1.4. Побудова моделі реалізації загроз безпеки в КМіС

Моделювання процесу реалізації загроз КМіС доцільно здійснювати на основі розгляду логічного ланцюжка: “загрози – джерело загрози – метод реалізації – уразливість – наслідки”. На рис. 13.7 подана структурна схема моделі реалізації загроз інформаційних ресурсів у КМіС.

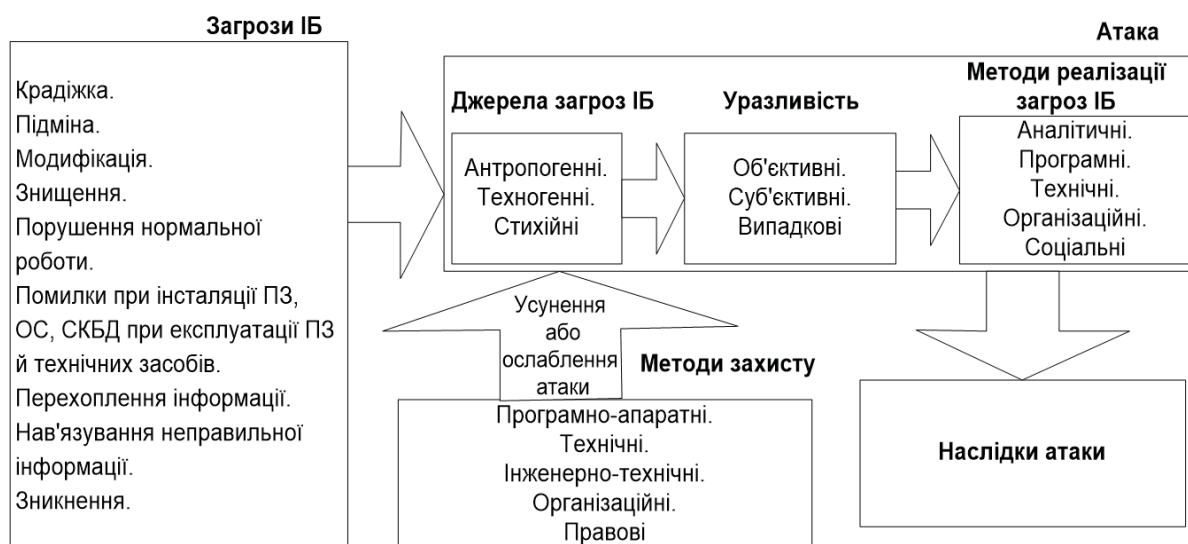


Рис. 13.7. Структурна схема моделі реалізації загроз інформаційних ресурсів в КМіС

Аналіз негативних наслідків реалізації загроз припускає обов'язкову ідентифікацію (наприклад, присвоєння унікального коду) можливих джерел загроз, уразливостей, що сприяють їх прояві та методів реалізації, тобто класифікацію (рис. 13.8).

Для опису моделі реалізації загроз інформаційних ресурсів зафіксуємо кінцеву множину суб'єктів, взаємодіючих з інформаційною системою – S , параметр N – кількість уразливих до атаки комп'ютерів (ПК); параметр D містить початкове значення середньої кількості атакованих комп'ютерів за

обрану одиницю часу. Вважаємо, що D є константою, обчислення враховують, що комп'ютер не може бути атакований двічі; $a(t)$ – пропорція вразливих ПК, які були успішно атаковані за час t , $N \cdot a(t)$ – загальна кількість успішно атакованих комп'ютерів, за час t зроблено не більше $D(1 - a(t))$ нових успішних атак. Кількість захоплених комп'ютерів за період часу $d(t)$ дорівнює:

$$n = aN \cdot D(1 - a)dt.$$



Рис. 13.8. Мета і загрози безпеки інформації

Враховуючи, що N – константа і $n = d(Na) = Nda$, правильне таке рівняння:

$$Nda = aN \cdot D(1 - a)dt,$$

у диференціальному вигляді:

$$\frac{da}{dt} = Da(1 - a),$$

має таке рішення:

$$a = \frac{e^{D(t-T)}}{1 + e^{D(t-T)}},$$

де T – часовий параметр, що характеризує найбільше зростання атак.

Для побудови загальної структури підсистеми безпеки інформаційної безпеки в КМіС і моделей атак обраний функціональний тип математичних моделей, який називається моделями “чорної скриньки”. Математична модель є моделлю об’єкта, процесу або явища, що становить математичні закономірності, за допомогою яких описані основні характеристики об’єкта, який моделюємо, процесу або явища [16]. Загальним для опису даних математичних моделей є процес формування криптограми.

Для цього зафіксуємо кінцеву множину $I = \{I_1, I_2, \dots, I_m\}$ переданих пакетів, причому кожному пакету відповідає ймовірність $P^*(I_j)$. Розподіл ймовірностей випадкового процесу задається сукупним розподілом ймовірностей випадкових величин, тобто множиною ймовірностей $P^*_o = \{P^*(I_1), P^*(I_2), \dots, P^*(I_m)\}$. Джерело ключів породжує потік ключів з множини K і/або K^* . Кожному ключу $K_i \in K = \{K_1, K_2, \dots, K_k\}$ відповідає деяка ймовірність $P^*(K_i)$, а кожному $K_i^* \in K^* = \{K_1^*, K_2^*, \dots, K_k^*\}$ відповідає ймовірність $P^*(K_i^*)$. Випадковий процес вироблення ключів задається множиною ймовірностей:

$$P^*_K = \{P^*(K_1), P^*(K_2), \dots, P^*(K_k)\}$$

$$P^*_{K^*} = \{P^*(K_1^*), P^*(K_2^*), \dots, P^*(K_k^*)\}.$$

Вибір ключа K_i визначає конкретне відображення φ_i з множини відображень і криптограма формується: $E_l = \varphi_i(K_i, I_j)$.

Відмінність між активними і пасивними атаками полягає в тому, що при виконанні атак першого типу (активні атаки) порушник здійснює активні дії, тобто дії, пов’язані зі зміною потоку даних або зі створенням фальшивих потоків (імітація, відтворення, модифікація повідомлень або перешкоди в обслуговуванні). Метою другого типу атак (пасивні атаки) є одержання переданої інформації (розкриття вмісту повідомлень і аналіз потоку даних).

Оцінка ступеня ефективності атаки може бути здійснена за рахунок проведення аналізу даних, якими володіє противник, його можливостей та інших параметрів пасивних атак. Основним методом оцінки можливостей противника при атаці є створення моделей атак.

13.1.5. Побудова математичної моделі пасивних атак у КМіС

Пасивні загрози впливають із прослуховування (несанкціонованого зчитування інформації) і не пов'язані з якою-небудь зміною інформації [2; 9; 15; 20; 21; 24; 29; 31]. Суть атаки полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, перехоплює всі дані, які були передані каналом зв'язку. Тобто при передачі криптограми E_1 в вузлі приймання по деякому каналу порушник виконує моніторинг мережі.

При цьому порушник (криптоаналітик) зобов'язаний володіти всіма відкритими параметрами і даними, які використовуються суб'єктами s . У такому випадку криптоаналітик може провести криптоаналіз протоколу з метою визначення сеансових або довгострокових ключів, які використовуються суб'єктами-учасниками протоколу.

Криптоаналіз протоколу залежить від типу протоколу, кількості й типу ключів, математичного апарату, які використовуються в протоколі, й інших характеристик протоколу. Узагальнена модель пасивних атак подана на рис. 13.9 – 13.10.

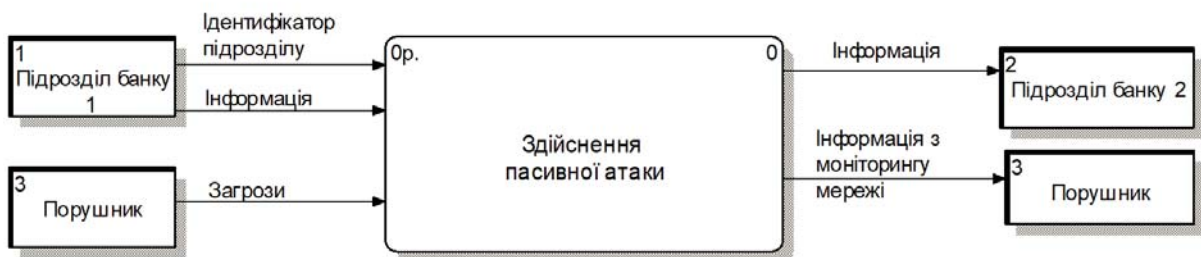


Рис. 13.9. Модель пасивних атак на інформаційні ресурси в КМіС

Криптоаналіз є рішенням математичного завдання з метою визначення самого повідомлення або деяких особистих ключів суб'єктів-учасників протоколу.

13.1.6. Побудова моделі активних атак у КМіС із блокуванням передачі інформації

Суть атаки із блокуванням передачі інформації полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, блокує передачу інформації, у результаті чого криптограма не досягає прийомної сторони.

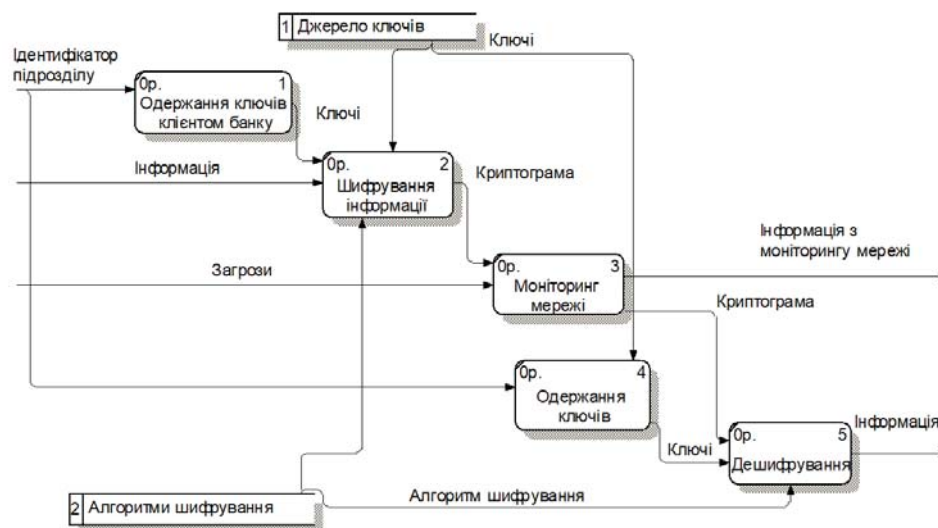


Рис. 13.10. Декомпозиція моделі пасивних атак

Узагальнена модель активних атак із блокуванням передачі інформації подана на рис. 13.11 – 13.12. Одержувачем інформації в даній моделі є порушник.

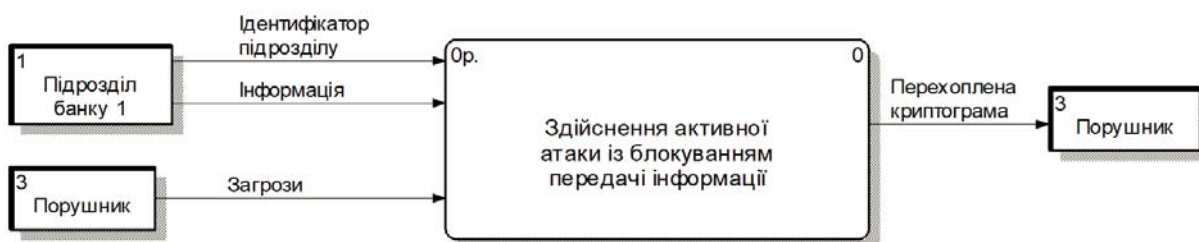


Рис. 13.11. Модель активних атак із блокуванням передачі інформації

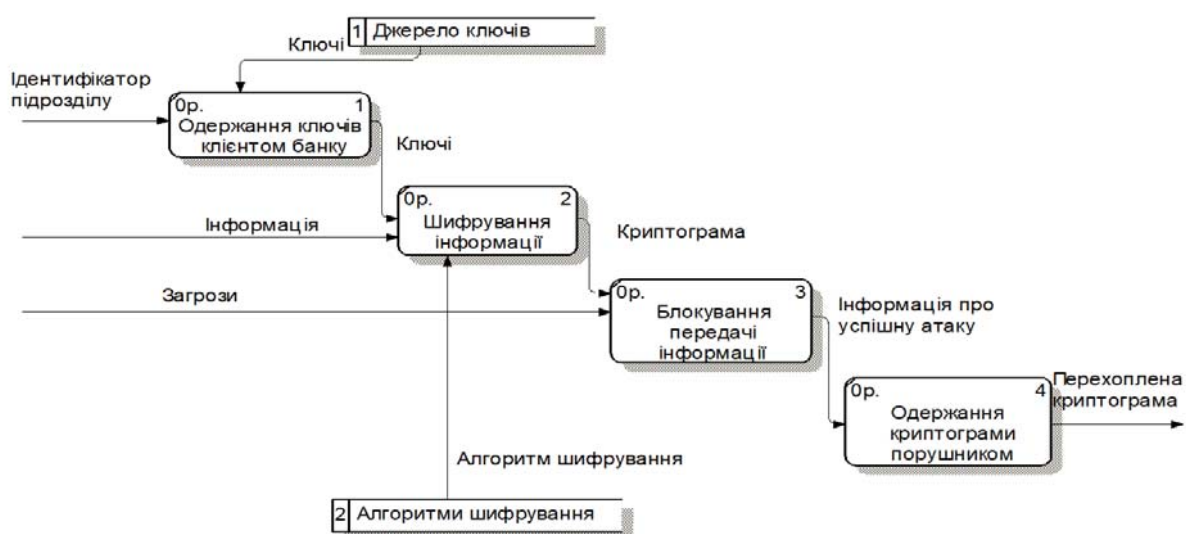


Рис. 13.12. Декомпозиція моделі активних атак із блокуванням передачі інформації

При реалізації даної атаки необхідні дані не досягають пункту призначення, або досягають занадто пізно, що призводить до втрати конфіденційної банківської інформації.

13.1.7. Побудова моделі активних атак у КМіС із внесенням перешкод

Суть атаки із внесенням перешкод полягає в тому, що порушник, визначивши факт виконання криптографічного протоколу, вносить деяку помилку e й передає в вузол приймання криптограму (E_{I+e}). На прийомному кінці за допомогою зворотного відображення φ_i^{-1} (заданого ключем K_i^*) із криптограми (E_{I+e}) відновлюється недостовірна інформація

$I_{je} = \varphi_i^{-1}(K_i^*, E_{I+e})$. Узагальнена модель активних атак із внесенням перешкод подана на рис.13.13 – 13.14.

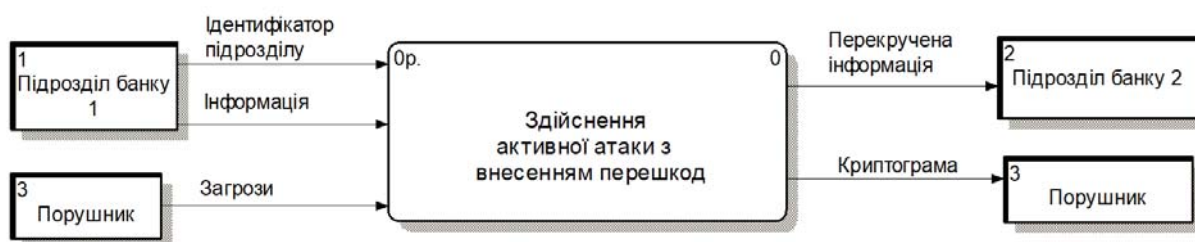


Рис. 13.13. Модель активних атак із внесення перешкод

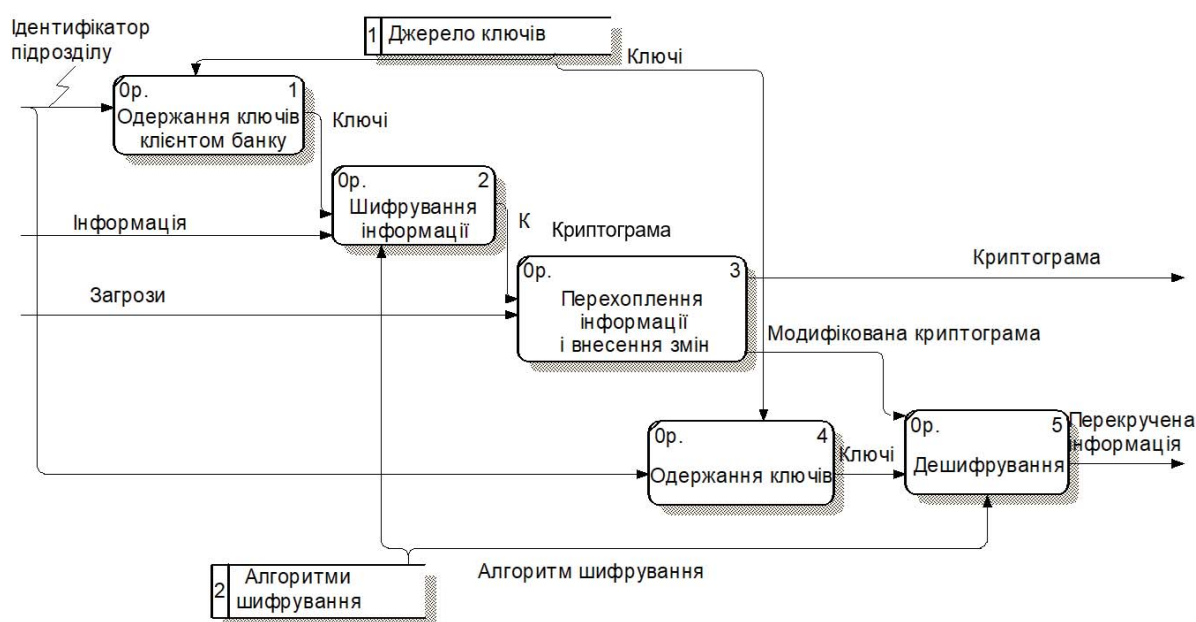


Рис. 13.14. Декомпозиція моделі активних атак із внесення перешкод

Реалізація даної атаки може призвести до збою або до одержання на прийомній стороні неправильної транзакції. Порушник може “керувати” конфіденційною інформацією, результатом цього є економічний збиток клієнтів КМіС.

13.1.8. Побудова моделі активних атак “маскарад” у КМіС

Суть атаки “маскарад” полягає в тому, що користувач (або інша сутність – процес, підсистема і т. д.) передає інформацію від імені іншого користувача. Способи заміни ідентифікатора можуть бути різні, зазвичай вони визначаються помилками та особливостями мережних протоколів. Проте на прийомному вузлі таке повідомлення буде сприйняте як коректне, що може призвести до серйозних порушень роботи КМіС.

Розглянемо процес виконання атаки даного типу. Порушник, визначивши факт виконання криптографічного протоколу, перехоплює криптограму E_l . З її допомогою він може спробувати обчислити апостеріорні ймовірності різних можливих повідомлень:

$$P^*_{o|E_l} = \{P^*(I_1|E_l), P^*(I_2|E_l), \dots, P^*(I_m|E_l)\};$$

і різних можливих ключів:

$$P^*_{K|E_l} = \{P^*(K_1|E_l), P^*(K_2|E_l), \dots, P^*(K_k|E_l)\},$$

які могли бути використані при формуванні криптограми E_l .

Множини апостеріорних ймовірностей утворюють апостеріорні знання порушника про ключі $K = \{K_1, K_2, \dots, K_k\}$ і про інформацію $I = \{I_1, I_2, \dots, I_m\}$ після перехоплення криптограми E_l . Фактично множини $P^*_{K|E_l}$ і $P^*_{M|E_l}$ є множинами припущень, яким приписані відповідні ймовірності. Одержавши необхідну інформацію, формує криптограму з недостовірною інформацією $E_{le} = \varphi_i(K_i, I_{je})$ і передає її на вузлі приймання.

На прийомному кінці за допомогою зворотного відображення φ_i^{-1} (заданого ключем K_i^*) із криптограми E_{le} відновлюється недостовірна інформація, передана порушником:

$$I_{je} = \varphi_i^{-1}(K_i^*, E_{le}), I_{je} \neq I_j.$$

Такого типу атака, як правило, пов’язана із спробами проникнення всередину периметра безпеки КМіС і часто реалізується хакерами.

Узагальнена модель активних атак “маскарад” подана на рис. 13.15, 13.16.

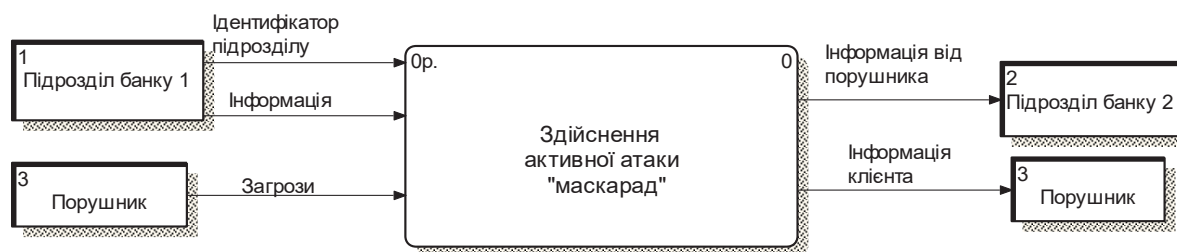


Рис. 13.15. Модель активних атак “маскарад”

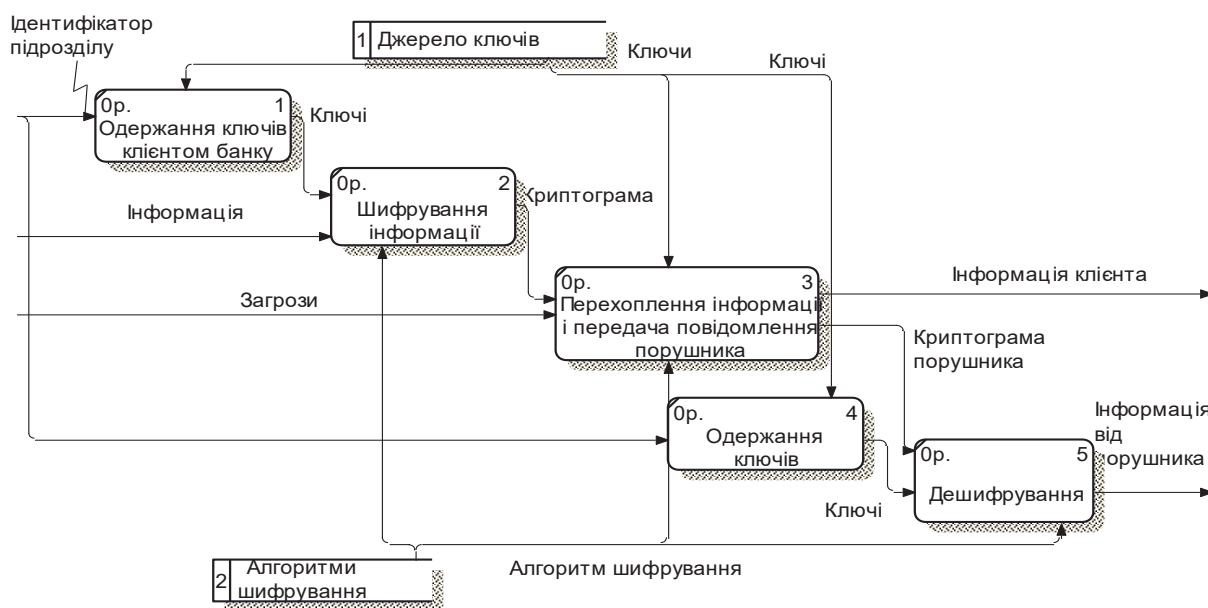


Рис. 13.16. Декомпозиція моделі активної атаки “маскарад”

При виконанні пасивної атаки порушник не впливає на протокол обміну інформацією в КМіС і намагається отримати інформацію про учасників протоколів за допомогою моніторингу мережі, тому пасивні атаки важко виявити. При активному розкритті криптопротоколів порушник намагається змінити протокол для власної потреби. Спроби виконання такого типу атаки переслідує більш широкий набір задач: отримання інформації, погіршення роботи системи або отримання несанкціонованого доступу до ресурсів.

Для побудови моделі безпеки на основі синергетичного підходу до оцінки загроз БІР, незалежно від складової безпеки (інформаційної безпеки (ІБ), КБ, безпеки інформації (БІ)) доцільно застосовувати принципи ризик-менеджменту, що дозволить при грамотному використанні основних його процедур своєчасно

визначити та класифікувати загрози, і, відповідно до ймовірності настання негативних наслідків від їх можливого прояву, адекватно організувати систему безпеки БІР.

Відзначається, що безпека інформації, в тому числі і банківської, може бути забезпечена лише при комплексному використанні всього арсеналу наявних засобів захисту у всіх структурних елементах виробничої системи і на всіх етапах технологічного циклу обробки інформації. Ігнорування методології системного аналізу при створенні систем безпеки БІР виходячи зі складності, а іноді і з неможливості об'єктивного підтвердження ефективності створених систем через недосконалість нормативно-методичного забезпечення безпеки, перш за все в області показників і критеріїв, так само створює перешкоди на шляху знаходження вирішення означеної проблеми.

Розвиток теорій ІБ, КБ, БІ на сучасному етапі пов'язаний з урахуванням нових обставин, характерних для сучасного періоду розвитку інформатизації суспільства на основі високих технологій. По-перше, оскільки все більшої актуальності набуває не тільки захист інформації, а й захист спільноти, особи і комунікаційних систем, в першу чергу, критичного застосування від руйнівного впливу інформації в кіберпросторі, то формується завдання забезпечення безпеки як органічної сукупності задач захисту інформації і захисту від інформації.

По-друге, від початку регулярного використання автоматизованих технологій обробки інформації актуальність завдання забезпечення необхідної якості інформації зростає, а саме завдання ускладнюється. Отже, еволюція обчислювальних технологій веде до виникнення емерджентних властивостей автоматизованих систем управління, а забезпечення безпеки неможливе без урахування завдань забезпечення якості інформації.

По-третє, рішення завдань захисту інформації, завдань захисту від інформації і забезпечення якості інформації обумовлює ефективність діяльності об'єктів. Виникає узагальнене поняття управління інформацією, що об'єднує вище означені поняття. У свою чергу, врахування завдань управління інформацією необхідний при формуванні, підтримці і використанні концепції інформаційного забезпечення діяльності об'єктів.

По-четверте, серйозну увагу на новому етапі розвитку теорії захисту інформації слід приділити вдосконаленню науково-методологічного базису та інструментальних засобів, що забезпечують вирішення будь-яких виникаючих завдань на регулярній основі в органічному зв'язку з вирішенням проблем інформаційної безпеки, інформаційних технологій, інформатизації суспільства.

Таким чином, усе сказане дозволяє виділити такі найактуальніші проблеми розвитку теорії та практики безпеки інформації:

- створення теоретичних основ і формування науково-методологічного базису, що дозволяють адекватно описувати процеси в умовах значної невизначеності та непередбачуваності прояву дестабілізуючих факторів (інформаційних загроз) при комплектованому синергетичному підході до їх оцінки в усіх складових поняття безпеки: ІБ, КБ, Бі;

- розробка науково-обґрунтованих нормативно-методичних документів у галузі безпеки БІР на основі вивчення та класифікації загроз інформації і вироблення стандартів вимог до захисту;

- стандартизація підходів до створення систем захисту інформації та раціоналізація схем і структур управління захистом на об'єктовому, регіональному та державному рівнях.

На рис. 13.17 наведено узагальнений підхід до побудови синергетичної моделі безпеки банківських інформаційних ресурсів.

На практиці найбільшого поширення набули два підходи до обґрунтування проекту підсистеми забезпечення безпеки.

Перший з них заснований на перевірці відповідності рівня захищеності ІС вимогам одного зі стандартів в області інформаційної безпеки. Це може бути клас захищеності відповідно до вимог профілю захисту розроблених відповідно до стандарту *ISO-15408*, або будь-який інший набір вимог. Тоді критерій досягнення мети в області безпеки – це виконання заданого набору вимог.

Критерій ефективності – мінімальні сумарні витрати на виконання поставлених функціональних вимог: $\sum c_i \rightarrow \min$, де c_i – витрати на i -й засіб захисту. Основний недолік цього підходу полягає в тому, що в разі, коли необхідний рівень захищеності жорстко не заданий (наприклад, через законодавчі вимоги) визначити “найбільш ефективний” рівень захищеності АБС досить складно.

Другий підхід до побудови системи безпеки БІР пов'язаний з оцінкою і управлінням ризиками на основі принципу “розумної достатності”. Однак, проведений аналіз показав, що дотримання балансу між витратами на захист і одержуваним ефектом, в т.ч. і економічним, що полягає в зниженні втрат від порушень безпеки носить суб'єктивний характер, і безпосередньо залежить від оцінки ризику загроз елементам АБС.

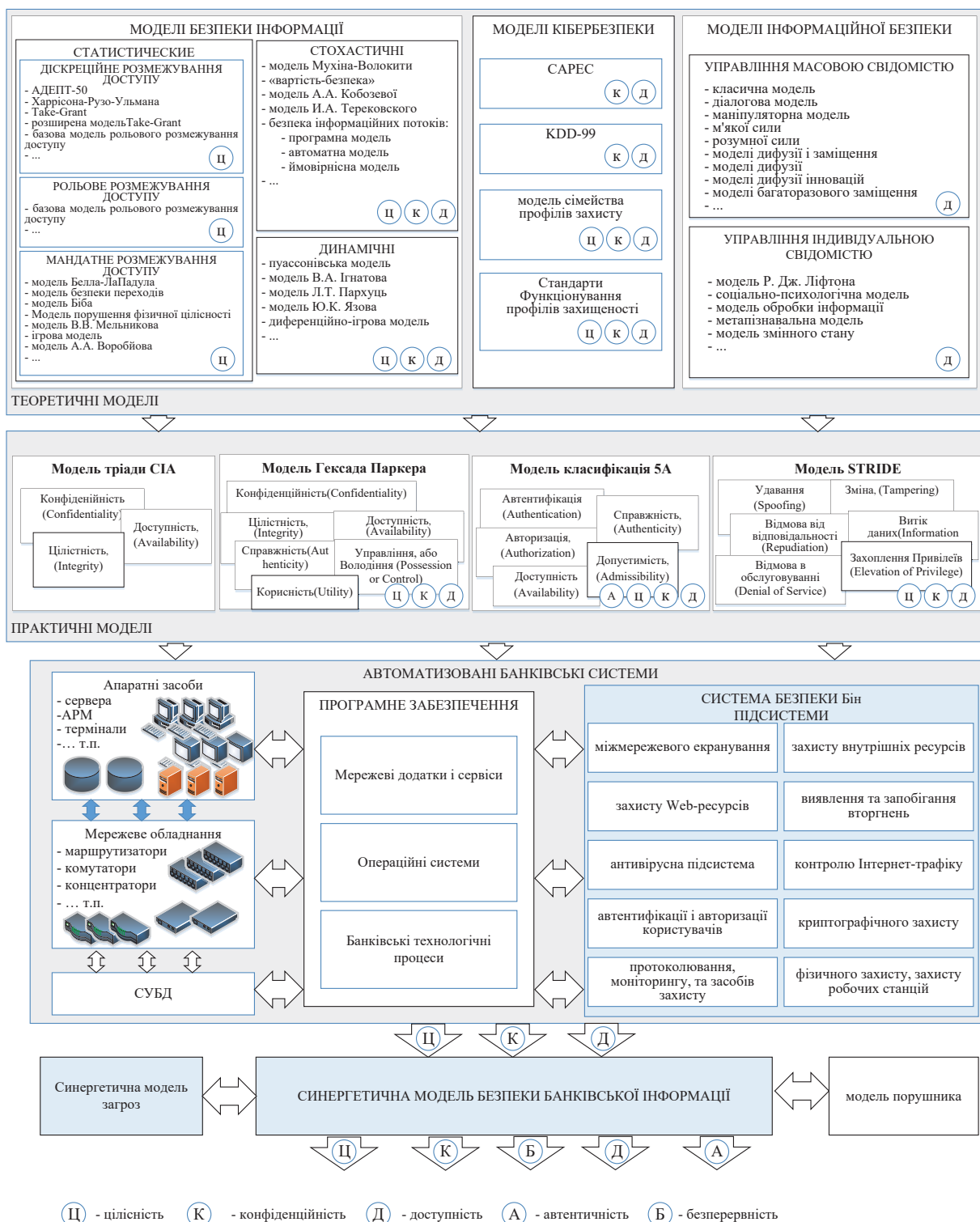


Рис. 13.17. Узагальнений підхід формування синергетичної моделі безпеки інформації на прикладі АБС ОБС

На основі аналізу визначимо дефініції безпеки інформації, основних механізмів і процедур, в рамках побудови моделі безпеки БІР на основі синергетичного підходу:

Банківські інформаційні ресурси (БІР) – інформація, що виникла в результаті банківської діяльності, а також відомості, що характеризують сам банк, його фінансове становище, надійність і виконання вимог законодавства.

Конфіденційність (confidentiality) – стан БІР, при якому інформація не може бути отримана неавторизованим користувачем і / або процесом.

Конфіденційність системи (system confidentiality) – властивість системи забезпечити захист БІР при передачі від пасивних атак.

Цілісність (integrity) – стан БІР, при якому інформація не може бути модифікована неавторизованим користувачем і / або процесом.

Цілісність системи (system integrity) – властивість системи забезпечити захист БІР при зберіганні, а також можливість модифікації БІР тільки авторизованим користувачем і / або процесом.

Доступність (availability) – стан БІР, при якому відсутні перешкоди доступу до інформації та закономірного її використання авторизованим користувачем і / або процесом.

Доступність системи (system availability) – властивість системи, яка полягає в тому, що авторизований користувач і / або процес, що володіє відповідними повноваженнями, може використовувати ресурс відповідно до правил, встановлених політикою безпеки, не чекаючи довше заданого (малого) проміжку часу, у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли вона йому необхідна.

Автентичність (authenticity) – стан БІР, при якому інформація забезпечує підтвердження автентичності джерела (авторизованого користувача і / або процесу) інформації.

Автентичність системи (system authenticity) – властивість системи, яка полягає в тому, що авторизований користувач і / або процес, що володіє відповідними повноваженнями, може підтвердити справжність джерела інформації.

Безперервність бізнес-процесів (business continuity) – властивість системи, яка полягає в забезпеченні безперебійної роботи внутрішніх і зовнішніх застосунків, дозволяє навантаженням і службам працювати без перерви під час запланованого простою і незапланованих збоїв, а також забезпечує резервне копіювання і зберігання критичних бізнес-даних і можливість їх відновлення протягом прийняттого періоду часу в випадку несподіваного інциденту або аварії.

Об'єкти загроз ІБ – відомості про склад, стан і діяльність банку (персоналу, матеріальних і фінансових цінностей, інформаційних ресурсів банку).

Загрози безпеки БІР – сукупність умов і факторів, що створюють загрозу несанкціонованого, в тому числі випадкового, доступу до банківських даних, результатом якого може стати знищення, зміна, блокування, копіювання, поширення БІР, а також інших НСД при їх обробці в АБС.

Загрози інформації виражаються в порушенні доступності, цілісності, автентичності та конфіденційності БІР.

Синергетичний показник безпеки БІР – синергетична оцінка ефективності комплексного застосування сил і засобів безпеки БІР в умовах антагоністичної протидії системи банківського захисту випадковим і цілеспрямованим загрозам безпеки.

Рівень захищеності банківських інформаційних ресурсів – якісний (кількісний) показник здатності системи захисту банківських інформаційних ресурсів АБС протистояти синергетичним і гібридним загрозам на складові безпеки: інформаційну безпеку, кібербезпеку, безпеку інформації.

Гібридність загроз ІБ, КБ, БІ – сукупність кількох загроз на банківські інформаційні ресурси за складовими безпеки: інформаційна безпека, кібербезпека, безпеку інформації, спрямованих на окрему послугу безпеки: конфіденційність, цілісність або автентичність, що дозволяє отримати максимальний ефект від їх комплексування.

Синергізм загроз ІБ, КБ, БІ – комбінований вплив декількох загроз на складові безпеки: інформаційну безпеку, кібербезпеку, безпеку інформації за послугами безпеки: конфіденційність, цілісність, автентичність, що характеризується тим, що їх об'єднана дія істотно перевершує ефект кожної окремо взятої загрози і їх простої суми.

Емерджентність АБС – сукупність особливих властивостей АБС, які не належать її підсистемам і блокам, а також сумі елементів, не пов'язаних особливими системоутворюючими зв'язками, на основі оцінювання синергізму і гібридності загроз складових безпеки (ІБ, КБ, БІ) на БІР, мінімізації витрат на інвестування в побудову системи безпеки БІР, забезпечення високої швидкості криптоперетворень та доказовий рівень стійкості в інтегрованих механізмах забезпечення цілісності, конфіденційності, автентичності і достовірності при використанні відкритих каналів зв'язку, оцінювання функціональної ефективності передачі БІР в АБС.

В узагальненому вигляді розглянуті компоненти наведені у вигляді концептуальної синергетичної моделі безпеки БІР на рис. 13.18.

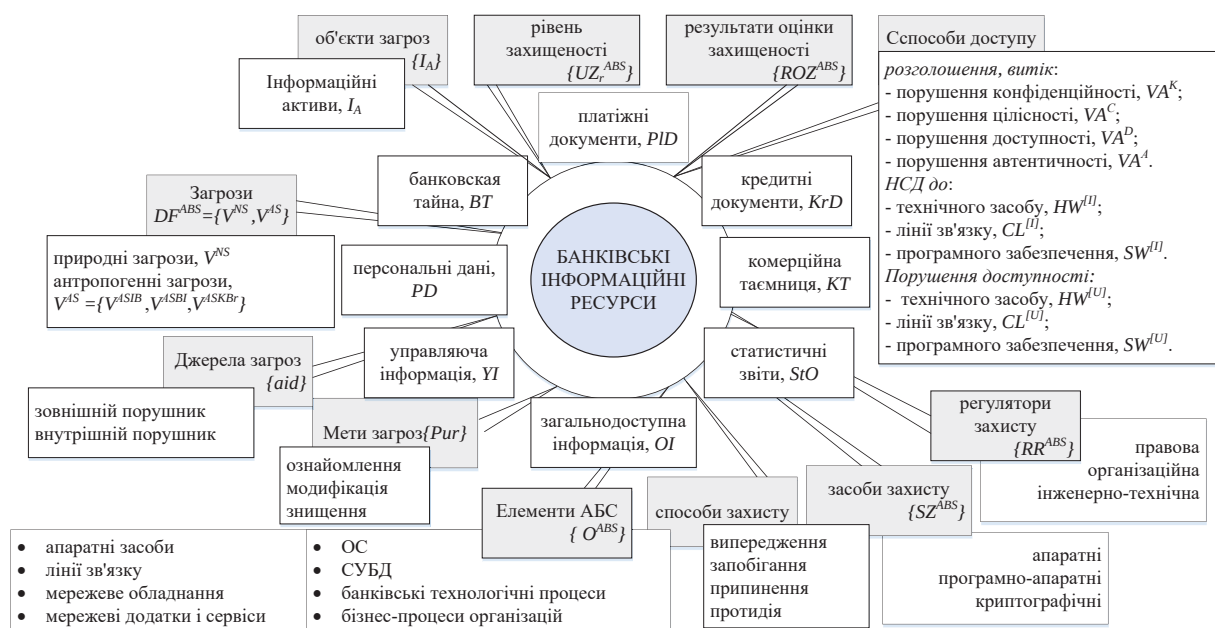


Рис. 13.18. Структурна схема концептуальної синергетичної моделі безпеки банківських інформаційних ресурсів

Джерелами загроз виступають конкуренти, зловмисники-хакери, бакери, інсайдери, тощо. Джерела загроз при цьому мають на меті: ознайомлення з БІР, їх модифікацію в корисних цілях і/або знищення для нанесення прямих матеріальних збитків.

Неправомірне заволодіння конфіденційною інформацією можливе за рахунок її розголошення, витоку БІР через технічні засоби та несанкціонований доступ до БІР.

Джерелами конфіденційної інформації є персонал, банківські процеси, документи, технічні носії БІР, технічні засоби забезпечення банківських транзакцій.

Основними напрямками захисту інформації є правовий, організаційний та інженерно-технічний захист інформації як виразники комплексного підходу до безпеки БІР.

Засобами захисту інформації є фізичні, апаратні, програмно-апаратні засоби і криптографічні методи.

Як способи захисту виступають організаційно-технічні заходи, способи і дії, що забезпечують упередження протиправних дій, їх запобігання, припинення та протидія несанкціонованому доступу до БІР.

Концептуальна синергетична модель безпеки БІР формується на основі методології та синергетичному підході до безпеки БІР, оцінювання рівня захищеності БІР ОБС України в умовах гібридизації загроз на складові безпеки (ІБ, КБ, БІ), а також часткових моделей: удосконаленої інфраструктурної моделі АБС, синергетичної моделі загроз, удосконалених моделі зловмисника і моделі оцінювання захищеності АБС.

Удосконалена інфраструктурна модель АБС являє собою таку формальну модель:

$$G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\},$$

де O^{ABS} – множина об’єктів середовища, що описують елементи АБС та їх приналежність до рівнів ієрархії АБС; L^{ABS} – множина зв’язків між елементами, визначається матрицею суміжності:

$$A^{ABS} = \|a_{ij}^{ABS}\|;$$

$\{I_A\}$ – множина елементів інформаційних активів БІР. Кожен елемент $I_A \in \{I_A\}$ описується вектором $I_A = (Type, A^C, A^D, A^A, A^K, C_Y)$. *Type* – тип інформаційного активу, описується множиною базових значень $Type = \{BT, PID, RrD, KT, StO, Ol, YI, PD\}$, де *BT* – банківська таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. A^K – конфіденційність; A^C – цілісність; A^D – доступність; A^A – автентичність; C_Y – безперервність – властивості інформації, які необхідно забезпечувати. Вони набувають значення 1 – якщо властивість необхідна, 0 – в іншому випадку.

Крок 1. Визначення зв’язку між інформаційними активами БІР $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS} = \|a_{ij}^{ABS}\|$.

Кожен елемент $I_A \in \{I_A\}$ описується вектором $I_A = (Type, A^C, A^I, A^A, A^{Au}, C_Y)$. *Type* – тип інформаційного активу, описується множиною базових значень $Type = \{BT, PID, RrD, KT, StO, Ol, YI, PD\}$, де *BT* – банківська таємниця; *PID* – платіжні документи; *KrD* – кредитні документи; *KT* – комерційна таємниця; *StO* – статистичні звіти; *Ol* – загальнодоступна інформація; *YI* – керівна інформація; *PD* – персональні дані. A^C – конфіденційність; A^I – цілісність; A^A – доступність; A^{Au} – автентичність; C_Y

– безперервність – властивості інформації, які необхідно забезпечувати. Вони набувають значення 1 – якщо властивість необхідна, 0 – в іншому випадку.

Крок 2. Визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами середовища. Кожен елемент $O_l \in \{O^{ABS}\}$ описується вектором $O_l = \{Y^{ABS}, IO\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною $Y^{ABS} = \{FL, NL, OSL, DBL, BL\}$, де FL – фізичний рівень; NL – мережевий рівень; OSL – рівень операційних систем (ОС); DBL – рівень систем управління базами даних; BL – рівень банківських технологічних застосунків і сервісів. Для визначення типу зв'язку та існуючого співвідношення IO^R між інформаційними активами БІР і об'єктами АБС використовується правило:

$$IO^R = \|IO_{il}^R\|,$$

де IO_{il}^R – відображає наявність і тип зв'язку між i -м інформаційним активом та l -м об'єктом середовища АБС. При цьому $\forall i \in \{I_A\}$, а $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^R = \begin{cases} 0 & \text{– зв'язок відсутній} \\ cs & \text{– включає і зберігає} \\ pt & \text{– обробляє або передає} \\ so & \text{– підтримує функціонування} \end{cases}.$$

Наступний крок – визначення комплексування множини загроз на основі синергетичної моделі загроз й узагальненої моделі зловмисника.

Крок. 3. Визначення комплексування множини загроз на основі синергетичної моделі загроз й удосконаленої моделі зловмисника.

Синергетична модель загроз формально описується виразом:

$$GR^{ABS} = \{\{DF^{ABS}\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\}.$$

Множина джерел загроз безпеці АБС представлена кортежем $DF^{ABS} = \{V^{NS}, V^{AS}\}$, в якому V^{NS} – клас природних джерел загроз, $V^{AS} = \{V^{ASIB}, V^{ASKB}, V^{ASBI}\}$ – клас антропогенних загроз, де V^{ASIB} – множина загроз інформаційній безпеці; V^{ASKB} – множина загроз кібербезпеці; V^{ASBI} – множина загроз безпеці інформації. T_{risk} – якісний показник ризику; T_P –

множина базових визначень ймовірності реалізації хоча б однієї загрози j -му активу; T_U – множина базових визначень величини збитку від реалізації загрози u_i ; VH – множина деструктивного стану елементів АБС, під яким розуміється небажаний і незапланований стан компонента АБС, в якому він опинився в результаті реалізації однієї або декількох загроз.

Для отримання синергетичного ефекту підвищення рівня захищеності БІР необхідно враховувати комплексування загроз:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\},$$

$$\text{де } \{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKB}\}.$$

Кожен елемент з множини загроз $DF_i \in \{DF^{ABS}\}$, може бути представлений таким вектором значень:

$$DF_i(p, u, risk),$$

де p – ймовірність реалізації загрози; u – потенційний збиток; $risk$ – ризик, виражений в якісній формі, що набуває один з двох станів: $T_{risk} = \{\text{допустимий, недопустимий}\} = \{\alpha_{r1}, \alpha_{r2}\}$.

Крок 4. Визначення ціни повного ризику всіх активів БІР. Ціна повного ризику дорівнює сумі цін ризику всіх активів:

$$R_{повн} = \sum_{j=1}^n R_j.$$

Крок 5. Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР. Розрахунок ймовірності реалізації хоча б однієї загрози для кожного активу виконується за виразом:

$$p_{rj} = 1 - \prod_{i=1}^m (1 - pr_{ij}),$$

де p_{rj} – ймовірність реалізації хоча б однієї загрози j -му активу.

Передбачається, що в разі реалізації для j -го активу хоча б однієї із загроз з множини $V^{AS} = \{V^{ASIB}, V^{ASBI}, V^{ASKBr}\}$, збиток дорівнює вартості активу на основі деталізації активів і ретельного вибору актуальних загроз:

$$q_j = u_j.$$

Вважається, що загрози можуть бути реалізовані незалежно один від одного, тоді ціна ризику R_j для кожного j -го активу визначається за виразом:

$$R_j = pr_j \times q_j.$$

Таким чином, ймовірність реалізації середовища p_{rj} , з областю визначення $P = [0, 1]$ задамо відповідно до множиною базових визначень $T_p = \{\text{нереалізована, мінімальна, середня, висока, критична}\} = \{\alpha_{x1}, \alpha_{x2}, \alpha_{x3}, \alpha_{x4}, \alpha_{x5}\}$.

Оцінка потенційно можливого збитку від реалізації загрози тісно пов'язана з капіталом і формується на основі експертних оцінок. Величина збитку від реалізації загрози u_i задається множиною базових визначень $T_U = \{\text{мінімальна, середня, висока, критична}\} = \{\alpha_{y1}, \alpha_{y2}, \alpha_{y3}, \alpha_{y4}, \alpha_{y5}\}$. Для визначення значення ризиків скористаємося правилом на основі системи нечітких висловлювань:

$$\tilde{L}^1 = \left\{ \begin{array}{l} \tilde{L}_1 : \langle E_{11} \cup E_{12} \cup E_{13} \cup E_{14} \cup E_{21} \cup E_{22} \cup E_{23} \cup E_{31} \cup E_{32} : risk_i \text{ є } \alpha_{r1} \rangle; \\ \tilde{L}_2 : \langle E_{24} \cup E_{33} \cup E_{34} \cup E_{42} \cup E_{43} \cup E_{44} \cup E_{51} \cup E_{52} \cup E_{53} \cup E_{54} : risk_i \text{ є } \alpha_{r2} \rangle \end{array} \right\}$$

де E_{kj} : " $p_{ri} \in \alpha_{xk}$ і $u_i \in \alpha_{yj}$ "

Практична значимість полягає у можливості своєчасного оцінювання взаємозв'язків між активами банківських інформаційних ресурсів, елементами інфраструктури, технічними засобами захисту автоматизованих банківських систем і можливими проявами загроз інформаційній безпеці, кібербезпеці та безпеці інформації, що дозволяє своєчасно корегувати керівні документи банку з інформаційної безпеки, планувати інвестування в технічні засоби захисту інформації, формувати превентивні заходи для недопущення реалізації загроз.

13.2. Життєвий цикл розробки систем безпеки

13.2.1. Розробка профілю захисту і проекту безпеки об'єкта оцінки

У 1999 році практично була закінчена розробка міжнародного стандарту ISO/IEC 15408 "Критерії оцінки безпеки інформаційних технологій", які ще відомі як "Єдині критерії" [29 – 31; 41; 47]. Єдині критерії – це погоджений стандарт, розроблений на основі наявних стандартів й інших нормативних документів з обліком накопиченого в різних країнах досвіду в галузі забезпечення безпеки інформації. Стандарт сприяє усуненню концептуальних і технічних розходжень, наявних у раніше розроблених документах [32; 42] і характеризує новий, міждержавний рівень стандартизації інформаційних технологій.

Однією з головних цілей стандарту є створення методологічної бази для здійснення оцінки властивостей безпеки продуктів і систем інформаційних

технологій (ІТ-продуктів і ІТ-систем). У цілому розробка даного документа спрямована на рішення завдання забезпечення безпеки інформаційних технологій (ІТ-безпеки).

При розгляді проблеми забезпечення ІТ-безпеки розроблювачі стандарту виходили з того, що є дві основні протидіючі (конфліктуючі) сторони – власник ресурсів, що представляє певну цінність і, отже, що вимагає свого захисту, і противник, що має мотиви й можливість для незаконного використання ресурсів, що може призвести до завдання збитків (морального, матеріального, економічного і т. д.) власнику ресурсів. При цьому під ресурсами (assets) розуміють не тільки інформацію (інформаційні ресурси), але й інші види ресурсів, наприклад, комунікаційні або обчислювальні ресурси. Порухник розглядається як джерело загроз безпеки (threat agent) – можливих подій, дій (впливів), процесів або явищ, що є потенційними небезпеками, реалізація яких може призвести до завдання збитків власнику ресурсів. У зв'язку із цим власник ресурсів змушений вживати заходів, які спрямовані на запобігання або зменшення ступеня цих небезпек. Як основні загрози розглядаються загрози порушення конфіденційності, цілісності і доступності. Однак для ефективної протидії противнику власник ресурсів повинен скласти якомога більш повний перелік загроз, які можуть бути реалізовані в конкретних умовах. Аналіз ризику реалізації загроз здійснюється шляхом завдання моделі порушника й оцінки ймовірності реалізації тієї або іншої загрози. Отримані результати дозволяють сформулювати вимоги щодо забезпечення ІТ-безпеки, реалізація яких сприяє зменшенню ризиків до прийняттого рівня [32; 42; 47].

Вимоги ІТ-безпеки по суті містять у собі функціональні вимоги безпеки і вимоги адекватності. Функціональні вимоги безпеки визначають набір функцій безпеки, які необхідно реалізувати для забезпечення конфіденційності, цілісності і доступності. Щоб механізми безпеки і засоби захисту функції, безпеки, що реалізують, можна було визнати ефективними, потрібен високий ступінь упевненості в правильності їх вибору і надійності функціонування. Така впевненість досягається шляхом пред'явлення та реалізації вимог адекватності.

Основними об'єктами застосування вимог безпеки є ІТ-продукти і ІТ-системи. Під продуктом інформаційних технологій розуміється представлення кінцевому споживачу готового до використання апаратного, програмного або програмно-апаратного засобу (або сукупність таких засобів) обробки інформації. ІТ-продукт не призначений для автономної експлуатації й інтегрується в

ІТ-систему (автоматизована система обробки інформації), яка становить організаційно-технічну систему, що містить у собі:

- сукупність технічних засобів передачі і обробки інформації (ІТ-продуктів), об'єднаних у функціонально повний комплекс;
- сукупність методів і алгоритмів обробки інформації у вигляді відповідного програмного забезпечення;
- інформаційні та інші ресурси;
- персонал і користувачів, об'єднаних за організаційно-структурним, тематичним, технологічним й іншими принципами для здійснення автоматизованої обробки інформації.

Практична реалізація вимог ІТ-безпеки виражається в розробці продукту або системи захисту інформації. У термінах ISO/IEC 15408 такими є об'єкт оцінки (TOE – Target of Evaluation) – ІТ-продукт або система, а також пов'язана з ними експлуатаційна, технічна, користувацька та інша документація, яка є основним об'єктом перевірки і оцінки [42; 47].

Таким чином, прийняті власником ресурсів заходи призводять до розробки об'єкта оцінки і визначають політику безпеки об'єкта оцінки, тобто множину правил, які регулюють порядок управління, використання, захисту і розподілу оцінки ресурсів, що захищені об'єктом.

Основними документами, що характеризують об'єкт оцінки з погляду забезпечення ІТ-безпеки, є профіль захисту (protection profile) і проект забезпечення безпеки (security target). Розглянемо порядок розробки цих документів.

13.2.2. Порядок розробки профілю захисту і проекту забезпечення безпеки

Профіль захисту (ПЗ) – це реалізаційно-незалежна множина функціональних вимог безпеки та вимог адекватності, спрямованих на задоволення потреб споживача. Профіль захисту є нормативним документом, що регламентує всі аспекти безпеки ІТ-продуктів і систем у вигляді сукупності функціональних вимог і вимог адекватності, пропонує функціям безпеки і, отже, до засобів і механізмів захисту. Профіль захисту також може бути використаний для класифікації об'єкта оцінки.

Проект безпеки (ПБ) становить множину вимог безпеки та специфікацій функцій безпеки. Проект безпеки використовується як основа для здійснення оцінки розглянутого об'єкта оцінки. Крім специфікацій

функцій безпеки і засобів захисту ПБ містить вимоги до сертифікації об'єкта оцінки та підсумкову специфікацію системи (підсистеми) забезпечення безпеки в конкретному ІТ-продукті або системі.

Розробка даних документів є основним практичним додатком Єдиних критеріїв. Розробка ПЗ і ПБ здійснюється, відповідно, у три і чотири етапи [32].

I етап. Аналіз безпеки середовища експлуатації об'єкта оцінки.

II етап. Визначення й формулювання завдань із забезпечення безпеки.

III етап. Розробка вимог ІТ-безпеки.

IV етап. Розробка специфікацій функцій безпеки й підсумкової специфікації забезпечення безпеки об'єкта оцінки.

Розглянемо більш докладно кожний із цих етапів.

Аналіз безпеки середовища експлуатації об'єкта оцінки здійснюється з метою:

- обмеження системи (підсистеми) забезпечення безпеки об'єкта оцінки від навколишнього середовища експлуатації;
- визначення ступеня небезпеки (агресивності) середовища експлуатації для функціонування об'єкта оцінки шляхом виявлення загроз безпеки і аналізу ризиків;
- формування вихідних передумов для визначення завдань із забезпечення безпеки;
- середовище експлуатації становить сукупність фізичних, інформаційних, технічних об'єктів і систем, зовнішніх стосовно об'єкта оцінки, а також організаційних заходів, правових норм, умов експлуатації і технологічних особливостей застосування об'єкта оцінки, що роблять фізичний, інформаційний, енергетичний та інший вплив на функціонування об'єкта оцінки. У середовище експлуатації також входять і можливі загрози безпеки, які вже існують або можуть виникнути в даному середовищі.

При здійсненні аналізу безпеки середовища експлуатації, з погляду забезпечення фізичної безпеки об'єкта оцінки, рекомендується звернути увагу на його фізичне оточення. При цьому аналізу піддаються фізичні засоби і міри забезпечення безпеки, у тому числі забезпечення фізичної безпеки персоналу.

Важливо врахувати ресурси, що вимагають свого захисту засобами об'єкта оцінки. Нарешті, аналіз здійснюється з урахуванням основного призначення об'єкта оцінки і того, чи є об'єкт оцінки ІТ-продуктом або ІТ-

системою. Якщо в якості об'єкта оцінки розглядається ІТ-продукт, то розроблювач може орієнтуватися лише на загальні припущення про середовище експлуатації, включаючи умови експлуатації, застосування і загрози безпеки. Така невизначеність пов'язана з тим, що ІТ-продукт розробляється в припущенні, що він буде використовуватися в багатьох системах обробки інформації. На відміну від ІТ-продукту ІТ-система розробляється для рішення конкретних прикладних завдань, розраховуючи на вимоги кінцевих споживачів (замовників). У цьому випадку розроблювач має можливість повною мірою враховувати специфіку впливів на об'єкт оцінки з боку середовища експлуатації.

Необхідно також розрізняти об'єкт оцінки з погляду його основного призначення. Залежно від того, яка головна мета функціонування об'єкта оцінки, необхідно переломлювати кут зору на аналіз середовища експлуатації об'єкта оцінки. Так у якості об'єкта оцінки можна розглядати продукт або систему, основним призначенням яких є забезпечення безпеки інформації або інших ресурсів. З іншої сторони, в якості об'єкта оцінки можуть виступати і комунікаційні системи, обчислювальні мережі, елементи систем передачі даних і здійснення електронних платежів і т.д.

У таких системах забезпечення безпеки є одним з множини функціональних завдань, спрямованих на досягнення головної мети функціонування.

Результатами аналізу безпеки є [32]:

1) аксіоматичні висновки (припущення) про безпеку середовища експлуатації конкретного об'єкта оцінки;

2) перелік загроз безпеки, оцінка ймовірності їх реалізації і модель порушника безпеки. Кожна загроза характеризується з трьох сторін. По-перше, визначається модель порушника безпеки, що здатний реалізувати конкретну загрозу; по-друге, описуються передбачувані методи нападів (атак) і можливі слабкі місця (уразливості) системи, використання яких лежить в основі реалізації атак. Нарешті, визначаються ресурси, які є об'єктом конкретної атаки. Все це є основою для проведення аналізу ризиків реалізації кожної загрози, що дозволяє оцінити ймовірність загрози та можливий збиток, що може бути нанесений у випадку реалізації загрози. Особливо зупинимося на моделі порушника. Тут необхідно виходити з того, якими ресурсами володіє потенційний противник, а також які мотиви для здійснення злочинних дій. У загальному випадку в ролі противника можна розглядати фізичну особу, що здійснює нерегулярні атаки, корпоративну

групу, що володіє обмеженими можливостями та ресурсами і державну спецслужбу, що володіє великими можливостями;

3) висновки щодо застосовності організаційної політики безпеки. Під *організаційною політикою безпеки* розуміють одне або декілька правил, процедур, практичних заходів (дій) або загальних рекомендацій, спрямованих на забезпечення безпеки і експлуатації об'єкта оцінки накладаються організацією відповідно до виконуваних даною організацією функцій. Тобто, організаційна політика безпеки є конкретизацією загальної політики безпеки об'єкта оцінки стосовно конкретної організації.

Таким чином, всі роботи, виконувані на даному етапі, спрямовані на забезпечення максимального обліку конкретних умов експлуатації об'єкта оцінки при його перевірці й оцінці.

На основі отриманих у ході аналізу безпеки середовища експлуатації результатів здійснюється визначення і формулювання задач із забезпечення безпеки або задач захисту (security target).

Задача захисту – це цільова постановка задачі на протидію виявленим загрозам і задоволення політики безпеки. Задача захисту повинна бути погоджена з множиною інших функціональних задач об'єкта оцінки і не суперечити основному призначенню об'єкта оцінки. Задачі визначаються як для об'єкта оцінки, так і для середовища його експлуатації. Причому останні формулюються тільки для елементів середовища експлуатації, пов'язаних з інформаційними технологіями. Технічні засоби забезпечення безпеки, організаційні міри, правові норми розглядаються як зовнішні стосовно об'єкта оцінки елементи системи захисту, застосовувані для підвищення ефективності власних засобів забезпечення безпеки об'єкта оцінки.

Таким чином, задача захисту адресована винятково для реалізації вимог забезпечення ІТ-безпеки.

Сформульовані і, по можливості, формалізовані задачі захисту є базою для безпосередньої розробки профілю захисту. Розробка профілю захисту здійснюється у два етапи:

- пошук і вибір профілю-прототипу;
- синтез вимог ІТ-безпеки.

Міжнародний стандарт передбачає створення спеціальної картотеки пакетів вимог безпеки, профілів захисту і проектів безпеки. *Пакетом вимог* називається проміжна комбінація вимог безпеки, що описує множину функціональних вимог і вимог адекватності, які забезпечують рішення виділеної підмножини задач захисту. Дана картотека буде доступна для

розроблювачів, що дозволяє мінімізувати витрати на розробку нових профілів захисту і врахувати досвід попередніх розробок.

Вимоги ІТ-безпеки є уточненням, конкретизацією і відображенням задач захисту в множині вимог безпеки, пропонованих об'єкту оцінки і до середовища експлуатації. *Вимоги ІТ-безпеки* містять у собі три компоненти:

- функціональні вимоги безпеки;
- вимоги адекватності;
- вимоги безпеки середовища експлуатації.

У ході розробки профілю захисту здійснюється вибір вимог безпеки специфічних для конкретного середовища. При цьому вибір ґрунтується на оцінці ефективності вимог для рішення задачі протидії загрозам безпеки [32].

Функціональні вимоги визначають властивості безпеки і характеризують функції об'єкта оцінки, які є типовими для підтримки ІТ-безпеки.

Декомпозиція даних вимог, їх опис приводиться в другій частині ISO/IEC 15408-2, що є каталогом функціональних вимог [56 – 58].

Демонстрація того, що виконання функціональних вимог веде до забезпечення необхідного рівня безпеки, здійснюється через включення в профіль захисту вимог адекватності. Адекватність містить у собі два аспекти: ефективність функцій безпеки; коректність реалізації функцій безпеки.

При оцінці ефективності функцій безпеки необхідно визначити ступінь відповідності між завданнями захисту й пропонованим набором функцій безпеки, їх функціональною повнотою, погодженістю, простотою використання і ступенем запобігання загроз безпеки. Коректність виражається в оцінці правильності та надійності реалізації функцій безпеки.

Для конкретної множини функціональних вимог ступінь адекватності може варіюватися. Тому адекватність виражається через рівні строгості вимог адекватності. Третя частина стандарту вводить шкалу рівнів оцінки адекватності, що опирається на вимоги адекватності.

При розробці профілю захисту необхідно аналізувати зв'язки і взаємозалежності як між різними функціональними вимогами, так і між функціональними вимогами і вимогами адекватності.

Вимоги безпеки, в остаточному підсумку, повинні демонструвати як наявність бажаних характеристик і властивостей безпеки, так і відсутність небажаних характеристик. Бажані характеристики можна продемонструвати через використання або тестування конкретного продукту, у той час як

визначення небажаних характеристик затруднено. Перевірка, моделювання, аналіз конструкції і реалізації профілю істотно знижує ризик присутності таких небажаних характеристик. Тому підсумком робіт з розробки профілю захисту є оцінка його повноти, коректності, несуперечності (погодженості) і реалізованості.

Четвертий етап здійснюється при розробці проекту безпеки. На даному етапі здійснюється розробка підсумкової специфікації об'єкта оцінки. Дана специфікація містить у собі опис заявлених функцій безпеки, які задовольняють функціональним вимогам і визначення показників адекватності, що характеризують ступінь задоволення вимог адекватності.

13.2.3. Структура і зміст профілю захисту

Згідно з ISO/IEC 15408-1 профіль захисту повинен містити в собі наступні розділи [52; 56 – 58]:

1. Короткий опис профілю.
2. Короткий опис об'єкта оцінки.
3. Аналіз середовища експлуатації об'єкта оцінки.
4. Завдання із забезпечення безпеки.
5. Вимоги IT-безпеки.
6. Обґрунтування завдань захисту і вимог IT-безпеки.

Короткий опис профілю містить класифікаційну інформацію, необхідну для його ідентифікації в спеціальній картотеці. Тут же характеризується основне завдання або група завдань із забезпечення безпеки, розв'язуваних за допомогою даного профілю.

Короткий опис об'єкта оцінки містить:

- призначення і область застосування об'єкта оцінки;
- короткий опис особливостей, використовуваних у об'єкті оцінки інформаційних технологій;
- короткий опис додатків, у яких передбачається використання об'єкта оцінки (у випадку, якщо основним призначенням об'єкта оцінки є забезпечення безпеки інформації та інших ресурсів).

Розділ аналіз середовища експлуатації містить результати аналізу безпеки середовища експлуатації об'єкта оцінки й містить у собі:

- а) висновки щодо різних аспектів безпеки середовища, в якому застосовується або передбачається застосування об'єкта оцінки, а саме:

- відомості про передбачуване використання об'єкта оцінки, включаючи відомості про додатки, ресурси і обмеження на використання;

- відомості про середовище експлуатації об'єкта оцінки, включаючи фізичні, інформаційні, технічні, технологічні, експлуатаційні й інші аспекти;

б) повний опис загроз безпеки, які безпосередньо впливають на безпеку об'єкта оцінки. Загрози описуються з погляду:

- противника, здатного реалізувати загрозу (модель противника, доступні ресурси для здійснення злочинних дій, мотиви здійснення злочинних дій);

- атак (методи нападів, використовувані слабкі місця системи захисту й інших сприятливих умов для реалізації конкретної атаки);

- ресурсів, що захищаються.

в) опис організаційних політик безпеки.

У розділі завдання із забезпечення безпеки докладно описуються завдання захисту для об'єкта оцінки і його середовища експлуатації.

Завдання захисту повинні:

- відбивати конкретні цілі, що досягаються в ході забезпечення безпеки;

- бути застосованими для запобігання всіх виявлених загроз безпеки;

- охоплювати всі певні організаційні політики безпеки.

Розділ вимоги ІТ-безпеки містить опис функціональних можливостей засобів захисту об'єкта оцінки і визначає рівень адекватності пред'явлених функціональних вимог стосовно певного раніше переліку загроз безпеки.

Розділ містить у собі:

- функціональні вимоги безпеки для об'єкта оцінки;

- вимоги адекватності безпеки об'єкта оцінки;

- вимоги безпеки для ІТ-середовища експлуатації об'єкта оцінки.

При розробці даного розділу необхідно враховувати наступні умови:

- всі вимоги ІТ-безпеки формуються на основі використання другої і третьої частин стандарту ISO/IEC 15408 [56 – 58];

- формулювання функціональних вимог і вимог адекватності повинне бути зрозумілим і однозначним, що дозволяє в остаточному підсумку провести їх оцінку і продемонструвати погодженість вимог;

- якщо необхідно, використовувати для компонентів функціональних вимог встановлені операції над ними з метою дозволу або заборони використання конкретних механізмів безпеки;

– при синтезі функціональних вимог і вимог адекватності враховувати всі взаємозв'язки й взаємозалежності між ними.

Нарешті в розділі обґрунтування задач захисту і вимог ІТ-безпеки представляються докази того, що профіль захисту становить повну і зв'язну множину вимог до об'єкта оцінки, що задовольняє пред'явленим вимогам, забезпечує ефективну протидію загрозам безпеки. Розділ містить у собі наступні відомості:

а) обґрунтування завдань захисту, що демонструє, що заявлені завдання захисту відбивають і охоплюють всі аспекти безпеки об'єкта оцінки і середовища експлуатації;

б) обґрунтування вимог безпеки, що демонструє, що множина вимог безпеки (і для об'єкта оцінки, і для середовища експлуатації) застосована для реалізації всіх завдань захисту. При цьому:

– комбінація окремих функціональних вимог і вимог адекватності задовольняє конкретним завданням захисту;

– повна множина вимог безпеки утворює взаємно підкріплювальне і внутрішньо погоджене ціле;

– вибір вимог безпеки є виправданим. Крім того виправданим повинен бути вибір вимог, що не втримуються в стандарті ISO/IEC 15408, вибір рівня адекватності, не представленого в шкалі встановлених рівнів, а також незадоволення яких-небудь залежностей між вимогами;

– обраний рівень захищеності погоджений із задачами захисту.

Крім перерахованих вище розділів профіль захисту може містити додаткові відомості щодо конструкції, оцінки й застосування об'єкта оцінки.

13.2.4. Структура і зміст проекту з забезпечення безпеки

Розробка проекту безпеки опирається на один або декілька профілів захисту. Тому структура і зміст ПБ схожі зі структурою і змістом профілю захисту. ПБ містить у собі вісім розділів.

1. Короткий опис проекту безпеки.
2. Короткий опис об'єкта оцінки.
3. Аналіз середовища експлуатації об'єкта оцінки.
4. Завдання із забезпечення безпеки.
5. Вимоги ІТ-безпеки.
6. Підсумкова специфікація об'єкта оцінки.
7. Необхідні профілі захисту.

8. Обґрунтування.

Перші п'ять розділів ПБ аналогічні за змістом відповідним розділам профілю захисту. Більш того, вони можуть бути повністю взяті з обраного профілю захисту.

Підсумкова специфікація об'єкта оцінки містить специфікації (технічний опис) функцій безпеки об'єкта оцінки, які охоплюють вимоги ІТ-безпеки й визначають, яким чином функції безпеки підтримують функціональні вимоги безпеки об'єкта оцінки. Специфікації подаються у вигляді двохстових таблиць, що відображають зв'язок між функціями і функціональними вимогами. Таке подання дозволяє чітко показати, яка функція спрямована на задоволення конкретної вимоги і що зазначена вимога задоволена. Крім того при подальшій формалізації опису функцій безпеки й функціональних вимог таке подання дозволить залучити засоби ЕВТ для аналізу проекту безпеки.

Функції безпеки визначають у неформальному вигляді з необхідним рівнем деталізації. При описі механізмів безпеки чітко вказують, для реалізації яких функцій безпеки використовується конкретний механізм. Нарешті, за необхідності, вказують рівень стійкості (захищеності) функції безпеки.

Стандарт визначає три рівні – базовий, середній і високий. Вибір рівня залежить від ступеня небезпеки загроз безпеки, на запобігання яких спрямована дана функція, і від моделі порушника. Необхідно представити доказ стійкості функції безпеки, що надалі допоможе експерту винести своє судження про адекватність і коректність обраного рівня стійкості функції безпеки.

Крім того даний розділ містить у собі формулювання показників адекватності, які характеризують ступінь задоволення вимог адекватності. У розділі “Необхідні профілі захисту” представляються відомості про ПЗ, на основі яких розробляється проект безпеки.

Нарешті, восьмий розділ містить обґрунтування завдань захисту, вимог безпеки, підсумкової специфікації об'єкта оцінки і вибору необхідних профілів захисту. В обґрунтуванні підсумкової специфікації об'єкта оцінки вказують, що функції безпеки об'єкта оцінки і показники адекватності застосовані для забезпечення вимог безпеки і показують, що:

- комбінація функцій безпеки об'єкта оцінки та їх спільне функціонування задовольняє функціональним вимогам безпеки;
- стійкість функцій безпеки об'єкта оцінки достатня;

– вибір показників адекватності виправданий і ці показники погодяться з вимогами адекватності.

Таким чином, проект безпеки становить, по суті, технічне завдання на розробку або оцінку безпеки конкретного продукту або системи, які реалізують функції забезпечення безпеки інформації та інших ресурсів.

13.2.5. Аналіз сучасних послуг й механізмів захисту інформації та визначення основних напрямків захисту КМіС

Стандарти ISO 7498-2 – Архітектура безпеки BBC і ISO/IEC 10181 – Основні положення безпеки мають загальний характер і висвітлюють питання безпеки інформації в комп'ютерних мережах [17; 32; 42; 58].

Проблема захисту комп'ютерних мереж від несанкціонованого доступу набула особливої гостроти. Розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значній відстані один від одного.

Все це викликає збільшення кількості вузлів мереж і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до мережі і доступу до важливої інформації [1; 2; 10; 12 – 14; 15; 20 – 24; 26 – 31; 36; 42; 47 – 51].

Загрози підрозділяються на навмисні (наприклад, атака з боку хакера) і випадкові (наприклад, посилка на неправильну адресу в результаті збоїв під час передачі повідомлення). Навмисні загрози підрозділяються на пасивні та активні.

Пасивні загрози впливають із прослуховування (несанкціонованого зчитування інформації) і не пов'язані з якою-небудь зміною інформації.

Активні загрози є наслідком спроб перехоплення і зміни інформації. Як правило, реалізація пасивних загроз вимагає менших витрат, ніж реалізація загроз активних.

Класифікуючи загрози, виділимо фундаментальні загрози, первинні ініціюючі загрози і базові загрози. Згідно з [15; 20; 23, 24, 47 – 51] до фундаментальних загроз відносяться:

Витік інформації – розкриття інформації неавторизованому користувачу або процесу.

Порушення цілісності – компрометація погодженості (несуперечності) даних шляхом цілеспрямованого створення, підміни або руйнування даних.

Відмова в послугі – навмисне блокування легального доступу до інформації або інших ресурсів (наприклад, за допомогою перевантаження сервера потоком запитів).

Незаконне використання – використання ресурсів незаконним чином. Використання ресурсів неавторизованим об'єктом або суб'єктом. Наприклад, використання вилученого комп'ютера з метою “зламу” інших комп'ютерів мережі.

Реалізація фундаментальних загроз багато в чому залежить від реалізації первинних загроз.

Первинні загрози ініціюють фундаментальні загрози розподіляються на загрози проникнення і загрози впровадження.

До загроз проникнення відносяться:

- *Маскарад* – користувач (або інша сутність – процес, підсистема та ін.) маскується і намагається видати себе за іншого користувача. Дана загроза, як правило, пов'язана зі спробами проникнення усередину периметра безпеки і часто реалізується хакерами.

- *Обхід захисту* – використання слабких місць системи безпеки для обходу захисних механізмів з метою одержання законних прав і привілеїв.

- *Порушення повноважень* – використання ресурсів не за призначенням. Дана загроза пов'язана з діями внутрішнього порушника.

До загроз впровадження відносяться:

- *Троянські програми* – програми, що містять схований або явний програмний код, при виконанні якого порушується функціонування системи безпеки. Приклад троянської програми – текстовий редактор, що окрім звичайних функцій редагування виконує таємне копіювання документа, що редагується, у файл противника.

- *Приховані ходи* – деякі додаткові можливості, які вбудовуються таємно в систему або її компоненти, що порушують функціонування системи безпеки при введенні специфічних даних. Наприклад, підсистема login може пропускати запит і перевірку пароля при уведенні певного ім'я користувача. Аналіз більше трьох тисяч комп'ютерних злочинів показав, що найчастіше виникали наступні загрози (у порядку убудування): порушення повноважень; маскарад; обхід захисту; троянські програми або приховані ходи; “копання в інформаційному смітті”.

Відомо, що в мережному вірусі Internet Worm була реалізована комбінація обходу захисту і маскараду.

Для обходу захисту розроблювачі вірусу скористалися слабкими місцями в системі безпеки ОС, а маскарад був реалізований шляхом вгадування паролів за допомогою спеціальної процедури. Проблема захисту комп'ютерних мереж від несанкціонованого доступу останнім часом придбала особливу гостроту.

Розвиток комунікаційних технологій дозволяє будувати мережі розподіленої архітектури, що поєднують велику кількість сегментів, розташованих на значному віддаленні один від одного. Все це викликає збільшення числа комутаційних вузлів і кількості різних ліній зв'язку між ними, що, у свою чергу, підвищує ризик несанкціонованого підключення до комутуючих елементів мережі і доступу до важливої інформації.

Проведений аналіз [10; 12; 13; 15; 20; 47 – 51] показав, що внутрішні загрози є однією з найбільш актуальних проблем інформаційної безпеки. Відповідно до статистики неправомірні дії співробітників самих організацій заподіюють найбільший збиток і до 90 % засобів, які виділяються на інформаційну безпеку, витрачається на забезпечення захисту від внутрішніх атак.

Неправомірні дії користувачів приведуть до значного збитку і підрозділяються на порушення конфіденційності даних, крадіжку інформації, перекручування інформації, дії, що приводять до збоїв інформаційних систем і втрату інформації.

Лідируючу позицію займають порушення конфіденційності даних, що приводять до витоку закритої інформації. За відомостями фахівців [10; 12; 13; 15; 20; 47 – 51] зі 100 випадків неправомірних дій співробітників 65 відносяться до порушення конфіденційності даних. Найпоширенішими шляхами витоку інформації є електронна пошта (до 22 %), інтернет (сайти, чати, форуми, безкоштовні поштові сервіси) до 20 %, інтернет-пейджери (ICQ/AOL, AIM, MSN, Yahoo!) і мобільні накопичувачі (компакт-диски, USB-накопичувачі) до 19 %, друкувальні пристрої до 8 % та інші джерела до 12 %. Слід зазначити, що можливості реалізації навмисних загроз останнім часом різко зросли через стрімкий розвиток обчислювальної техніки, і так званих суперкомп'ютерів, широким поширенням технологій розподілених обчислень. Аналіз наведених даних показує, що обчислювальні можливості окремих суперкомп'ютерів будуть перевищувати $3 \cdot 10^8$ GFLOPS, що дозволить розкривати ключі методом тотального перебору довжиною до 80 біт. Для запобігання ненавмисних і навмисних загроз необхідні спеціальні засоби ідентифікації користувачів у мережі, що забезпечують доступ до інформації лише у випадку повної впевненості в наявності у користувача прав доступу до неї.

13.3. Національні і міжнародні стандарти криптографічного захисту інформації в ІС

13.3.1. Рекомендації стандарту ISO 7498-2

Стандарт ISO 7498-2 (1989 року) присвячений питанням безпеки комп'ютерних мереж, побудованих на основі моделі взаємодії відкритих мереж (ЕМВС). Стандартом викладені результати аналізу існуючих загроз безпеки комп'ютерних мереж, вводиться спеціальна термінологія для опису послуг і механізмів безпеки, приводяться рекомендації з контролю й оцінки пропонованих засобів забезпечення безпеки мереж, а також визначається концепція управління безпекою. Даний документ розроблявся в тісному зв'язку з моделлю ЕМВС, і містить практичні рекомендації, які послуги безпеки можуть бути реалізовані конкретними протоколами на кожному рівні моделі ВВС, який механізм безпеки може бути використаний для реалізації конкретної послуги безпеки.

Розробники документа виходили з того, що існує визначений життєвий цикл розробки системи безпеки, який складається з п'яти етапів:

Визначення політики безпеки, що містить абстрактний ряд вимог до безпеки системи.

Аналіз вимог безпеки, включаючи аналіз ризиків, аналіз урядових, правових і стандартних вимог.

Визначення послуг безпеки, необхідних для задоволення пред'явлених вимог.

Побудова і впровадження системи безпеки, включаючи вибір механізмів безпеки, що забезпечують конкретні обрані послуги безпеки.

Безперервне управління безпекою.

У контексті моделі ISO/OSI життєвого циклу системи безпеки можна сказати, що загрозою безпеки є будь-що (дія, бездіяльність, засіб і т. д.), що сприяє порушенню політики безпеки і зламу системи безпеки (наприклад, втраті цілісності або конфіденційності). Послуга безпеки вибирається для забезпечення захисту від ідентифікованої загрози і становить абстрактні поняття, які можуть бути використані для характеристики вимог безпеки, а механізм безпеки є засобом, шляхом використання якого реалізується і застосовується послуга.

Важливо відзначити відмінність між послугою безпеки, що визначена для системи, і механізмом безпеки, що забезпечує реалізацію послуги. Наприклад, конфіденційність є послугою безпеки, а шифрування – механізмом, що використовується для забезпечення конфіденційності. Шифрування в той же час може використовуватися для реалізації інших послуг, наприклад, послуги автентифікації, а конфіденційність може бути забезпечена шляхом застосування інших механізмів, наприклад, засобами фізичного захисту даних.

У будь-якій системі безпеки правила, що визначають режим безпеки, повинні бути чітко представлені у вигляді політики безпеки. ISO 7498-2 визначає політику безпеки як “множина задокументованих правил забезпечення і впровадження послуг безпеки”. Іншим фундаментальним поняттям є поняття домену безпеки, під яким розуміють обмежену групу об’єктів і суб’єктів безпеки, керованих загальним адміністратором безпеки і до яких застосовується єдина політика безпеки. Політика безпеки є активним компонентом захисту, що включає в себе аналіз можливих загроз і вибір дій протидії загрозам.

Концепція архітектурних засобів безпеки ISO включає п’ять основних компонентів:

- визначення послуг забезпечення безпеки;
- визначення механізмів безпеки;
- рівневу модель побудови послуг забезпечення безпеки;
- співвіднесення послуг забезпечення безпеки і рівневої моделі;
- співвіднесення механізмів забезпечення безпеки і послуг.

Основою визначення переліку послуг забезпечення безпеки є наступні принципи побудови рівневої моделі безпеки:

Кількість альтернативних способів забезпечення безпеки повинна бути мінімізована. Ця вимога спрямована на мінімізацію вартості як самих послуг, так і додатків на їх основі.

Послуги забезпечення безпеки можуть працювати більше ніж на одному рівні моделі при побудові безпечної системи.

Функції засобів забезпечення безпеки не повинні дублювати існуючі аналогічні функції засобів комунікації.

Рекомендується не порушувати незалежність рівнів.

Кількість неконтрольованих (довірчих) функцій повинна бути мінімізована. Якщо який-небудь захисний механізм одного рівня базується

на використанні послуг більш низького рівня, то не повинно існувати ніяких проміжних рівнів, що забороняють або не гарантують такого зв'язку.

Послуги забезпечення безпеки, реалізовані на кожному рівні, повинні бути визначені таким чином, щоб допускати модульне доповнення до базових комунікаційних послуг.

13.3.1.1. Базові послуги безпеки

Стандарт ISO 7498-2 визначає п'ять базових послуг безпеки:

- автентифікація (authentication);
- управління доступом (access control);
- конфіденційність даних (data confidentiality);
- цілісність даних (data integrity);
- належність (причетність) (non-repudiation).

Розглянемо базові послуги більш докладно.

Автентифікація. Стандарт визначає два типи автентифікації: автентифікацію об'єкта (entity authentication) і автентифікацію джерела даних (origin authentication).

Автентифікація об'єкта комунікацій визначається як “підтвердження того, що об'єкт комунікації при з'єднанні саме той, котрий оголошений”. Ця послуга необхідна в системах із встановленням з'єднань і може застосовуватися періодично під час сеансу. Вона служить для запобігання таких загроз як маскарад і повтор попереднього сеансу зв'язку .

Автентифікація джерела даних допускає підтвердження того, що “джерело отриманих даних саме те, яке зазначене або оголошене”. Ця послуга істотна для комунікацій без встановлення з'єднання, для яких кожний пакет є незалежним від інших, і єдине, що може бути гарантоване, з погляду автентифікації, – це те, що джерело пакета саме те, яке зазначене у його заголовку. Функція не забезпечує захист від повторної передачі або модифікації даних.

Обидва види автентифікації визначені для мережного, транспортного й прикладного рівнів, на яких реалізуються протоколи з відновленням і без встановлення з'єднань.

Управління доступом. Дана послуга визначена як запобігання неавторизованого використання ресурсів, включаючи запобігання використанню ресурсів неприпустимим способом”. Тобто дана послуга забезпечує доступ до ресурсів тільки авторизованих користувачів (процесів), а

також гарантує тільки зазначені права доступу для авторизованих користувачів і запобігає неавторизований доступ як “внутрішніх”, так і “зовнішніх” користувачів. Ця послуга застосовується до різних типів доступу до ресурсів, наприклад, використання комунікаційних ресурсів, читання, запис або видалення інформаційних ресурсів, використання ресурсів обчислювальних систем з обробки даних і т. д. Дана послуга використовується для встановлення політики управління/обмеження доступу. Згідно з ISO 7498-2 політика управління доступом може визначатися критеріями ухвалення рішення про доступ або засоби, за допомогою яких регулюється доступ. Залежно від використовуваних критеріїв ухвалення рішення політика управління доступом може бути заснована на визначенні ідентичності явищ і об’єктів (identity-based) або правил (послідовності дій) доступу (rule-based) [58]. У першому випадку управління доступом засноване на використанні автентифікації для перевірки ідентичності суб’єкта доступу (користувача, процесу, проміжної або кінцевої системи) до надання йому доступу до ресурсів. У другому випадку політика управління доступом допускає ухвалення рішення про доступ на підставі послідовності правил, які співвідносять автентифікацію з точністю. Наприклад, правила можуть бути виражені в термінах часу і дати доступу або “благодійності”, що має даний користувач.

Стандарт визначає два типи політики управління доступом: обумовлена користувачем і обумовлена адміністратором. У більшості операційних систем (ОС) реалізований перший тип управління доступом. Другий варіант часто реалізується в мережах загального користування.

Конфіденційність даних. Конфіденційністю є “властивість, що гарантує, що інформація не може бути доступна або розкрита для неавторизованих (неуповноважених) осіб, об’єктів або процесів”. Питанням забезпечення конфіденційності приділяють велику увагу в тих системах, де розкриття інформації можливе в багатьох точках шляху передачі даних.

Для послуги визначені чотири типи:

- конфіденційність з’єднання забезпечує конфіденційність всіх даних користувача цього з’єднання;
- конфіденційність у режимі без встановлення з’єднання забезпечує конфіденційність всіх даних користувача в окремому блоці даних;
- конфіденційність виділеного поля даних призначена для захисту окремих інформаційних полів і вимагає, щоб тільки окремі поля в пакетах

були захищені. Даний тип послуги використовується як в мережах із встановленням з'єднання, так і в мережах без встановлення з'єднання;

- конфіденційність трафіку запобігає одержанню інформації шляхом спостереження (аналіз) трафіку. Це досягається шляхом захисту інформації про джерело – призначення, кількість переданих даних і частота передачі.

Цілісність даних. Захист цілісності даних має дві базові реалізації (для мереж із встановленням і без встановлення з'єднання), кожна з яких може застосовуватися для вибраних груп інформаційних полів. Захист цілісності даних в мережах із встановленням з'єднання допускає “виявлення будь-якої модифікації, включення, видалення або повторної передачі даних у послідовності (пакетів)”.

У мережах без встановлення з'єднання захист цілісності орієнтований на виявлення модифікацій кожного пакета без виконання аналізу великого обсягу інформації, наприклад, за сеанс або цикл передач. Ця послуга не запобігає навмисному видаленню, включенню або повторній передачі пакетів і доповнює автентифікацію джерела даних. Послуга захисту цілісності даних може додатково включати функції відновлення даних у випадках порушення їх цілісності.

Стандарт визначає п'ять типів послуги цілісності даних:

- цілісність з'єднання з відновленням забезпечує цілісність даних користувача цього з'єднання й виявляє будь-яку модифікацію, вставку, видалення або повторення даних з їх можливим наступним відновленням;

- цілісність з'єднання без відновлення аналогічна попередній послугі, але без можливості відновлення даних;

- цілісність виділеного поля в режимі із встановленням з'єднання забезпечує цілісність виділеного поля даних у пакеті користувача, переданих через це з'єднання;

- цілісність виділеного поля в режимі без встановлення з'єднання забезпечує цілісність виділеного поля в пакеті даних;

- цілісність блоку даних без з'єднання забезпечує цілісність окремого блоку даних (пакета). Орієнтована на виявлення тільки модифікацій і не запобігає навмисному видаленню, включенню або повторній передачі пакетів.

Причетність. У стандарті ISO 7498-2 [58] причетність визначається як “запобігання можливості відмови одним з реальних учасників комунікацій

від факту його повної або часткової участі в передачі даних”. Визначено дві форми причетності:

- причетність до посилки повідомлення (доказ джерела) надає одержувачу доказ того, що повідомлення було послано джерелом (на випадок відмови відправника від цього факту) і його цілісність не порушена;
- підтвердження (доказ) одержання повідомлень надає відправнику докази того, що повідомлення було отримане одержувачем, у випадку спроб останнього відмовитися від цього факту.

Відмінність послуги причетності від автентифікації полягає в тому, що одержувач або відправник даних може довести третій стороні (арбітрові, судді) факт передачі (одержання) даних і невтручання сторонніх у процес передачі даних. Доступність визначена як додаткова послуга забезпечення захищеності мереж. Механізми забезпечення доступності запобігають появам атак, що має своєю метою зробити ресурси або послуги комп’ютерної системи недоступними (або зробити їх “якість” незадовільним) для користувача.

Доступність є характеристикою якості ресурсу або послуги і частково визначається послугою управління доступом. Однак характер атак з метою обмеження доступу користувача й засоби боротьби з ними не ставляться безпосередньо до питань управління доступом. Тому доцільно виділити окрему послугу забезпечення доступності, що повинна реалізовуватися спеціальними механізмами на мережному рівні (наприклад, можливістю використання альтернативного шляху при атаці на доступну смугу основного каналу) або прикладному рівні.

13.3.1.2. Спеціальні механізми безпеки

Стандарт ISO 7498-2 [32; 58] містить короткий опис механізмів забезпечення безпеки й таблицю можливого співвідношення їх з рівнями моделі BBC і послугами. Механізми безпеки є конкретними мірами для реалізації послуг безпеки. Стандарт ділить механізми безпеки на два класи, а саме спеціальні механізми забезпечення безпеки, які використовуються для реалізації специфічних послуг і відрізняються для різних послуг, і загальні механізми, які не відносяться до конкретних послуг.

До спеціальних механізмів забезпечення безпеки відносяться наступні механізми:

- шифрування (encipherment);

- механізми цифрового підпису (digital signature mechanisms);
- механізми управління доступом (access control mechanisms);
- механізми забезпечення захисту цілісності даних (data integrity mechanisms), які включають криптографічні контрольні функції;
- механізми автентифікації (authentication exchange mechanisms);
- механізми заповнення трафіку (padding traffic mechanisms);
- механізми управління маршрутизацією (routing control mechanisms);
- механізми нотаризації (notarisation mechanisms).

Розглянемо кожний тип механізмів більш докладно.

Механізми шифрування. Шифрування допускає використання криптографічних перетворень даних для того, щоб зробити їх такими, що не читаються або не піддаються осмисленню. Шифрування застосовується разом зі зворотною функцією – розшифрування.

При шифруванні повідомлення M_i піддається крипто-графічному перетворенню F_k , у результаті чого формується криптограма:

$$C_i = F_k(M_i),$$

а розшифровування криптограми виробляється за правилом:

$$M_i = F_k^{-1}(C_i) = D_k(C_i),$$

де $k \in \{K\}_{N_{KL}}$ – ключ.

Використовується шифрування із симетричними (“закритими”, secret key) або несиметричними (“відкритими”, public key) ключами.

При симетричному шифруванні ключі шифрування й дешифрування однакові, тобто $K_{ш} = K_{расш}$. Симетричне шифрування має сенс тільки тоді, коли ключ не відомий іншим об’єктам, тобто коли він секретний.

При несиметричному шифруванні ключі шифрування й дешифрування різні, тобто $K_{ш} \neq K_{расш}$. У цьому випадку об’єкт генерує пари ключів, один із яких стає загальнодоступним або відкритим (public key), а другий зберігається об’єктом у таємниці з особистим ключем. При цьому знання відкритого ключа не дає можливості обчислити особистий ключ.

Шифрування використовується для забезпечення послуги конфіденційності, але може також підтримувати інші послуги забезпечення безпеки. Така можливість існує тому, що будь-яка зміна шифрограми

призводить до непередбачених змін вихідного тексту. При використанні шифрування можна також реалізовувати механізми забезпечення автентифікації та захисту цілісності даних. Відзначимо, що при використанні шифрування особливу значимість має завдання генерації, зберігання і поширення криптографічних ключів, що є окремим завданням управління безпекою.

Найбільш відомими алгоритмами шифрування, які є по суті стандартами де факто, є алгоритми DES і RSA. Після невдалих спроб стандартизувати DES і RSA на міжнародному рівні було ухвалене рішення, що механізми шифрування не будуть більше об'єктами стандартизації в ISO/IEC. Замість цього здійснюється тільки реєстрація алгоритмів. Порядок реєстрації визначений у стандарті ISO/IEC 9979 (1991 року). Хоча механізми шифрування і не є об'єктами стандартизації, міжнародний стандарт ISO/IEC 10116 (1997 року) (друга редакція) стандартизує режими роботи n-розрядних блокових симетричних алгоритмів шифрування.

Механізми цифрового підпису. Цифровий підпис є цифровим еквівалентом підпису (печатки, штампа та ін.), наявність якої в повідомленні дозволяє з високою точністю визначити джерело повідомлення (документа) і юридично довести, що з певною ймовірністю, тільки він міг створити й підписати цей документ.

Електронний цифровий підпис (ЕЦП) використовує “відкриті” ключі, генерується відправником даних і перевіряється одержувачем. Для шифрування контрольної суми повідомлення, що підписується, можуть бути використані методи несиметричного шифрування. ЕЦП складається із двох процедур: процедури накладання (генерації, формування) підпису й процедури зняття (перевірки, верифікації, деструкції) підпису.

Використання “відкритих” ключів для ЕЦП служить для підтвердження походження повідомлення, але не контролює одержувача повідомлення. ЕЦП використовується для забезпечення послуг автентифікації і захисту цілісності, для яких суб'єкт верифікації підписаних даних заздалегідь невідомий. При певному виборі контрольованого параметра цифровий підпис також може застосовуватися для реалізації послуги підтвердження причетності.

Основними стандартами ЕЦП є [15; 33]:

- міжнародний стандарт ISO/IEC 9796, який визначає ЕЦП з відновленням повідомлення (digital signature with message recovery);

- міжнародний стандарт ISO/ IEC 14888, який визначає ЕЦП з додаванням (digital signature with appendix);
- американський національний стандарт цифрового підпису (FIPS 186);
- американський фінансовий стандарт цифрового підпису з додаванням еліптичною кривою (ANSI X9.62);
- стандарт на ЕЦП PKCS #1, який визначає ЕЦП на основі алгоритму RSA;
- стандарт цифрового підпису з додаванням і відновленням повідомлення IEEE 1363 [54];
- стандарт цифрового підпису з додаванням еліптичної кривою IEEE P1363 [17];
- міжнародний стандарт ISO/IEC CD 15946-2 стандартизується ЕЦП еліптичною кривою з додаванням;
- державний стандарт України ДСТУ-4145 – 2002 [11].

На основі існуючих стандартів ЕЦП в [5; 11; 15; 30; 31; 32; 48; 54] запропонована класифікація ЕЦП.

За способом побудови схеми ЕЦП діляться на два класи:

- схема ЕЦП із відновленням повідомлення;
- схема ЕЦП із додаванням.

За кількістю учасників ЕЦП підрозділяється:

- одиночна схема ЕЦП;
- групова схема ЕЦП.

У процесі виконання алгоритму формування цифрового підпису в одиночних схемах ЕЦП досить одного учасника, у групових схемах їх два або більше.

За способом перевірки ЕЦП діляться на два класи:

- інтерактивні схеми ЕЦП, що вимагають протокольної взаємодії;
- неінтерактивні схеми ЕЦП, не потребуючі протокольної взаємодії.

Існуючі алгоритми ЕЦП можна розділити також за типами використовуваних односпрямованих функцій із секретом:

- схеми ЕЦП, засновані на стійкості факторизації великого числа;
- схеми ЕЦП, засновані на стійкості дискретного логарифма;
- схеми ЕЦП, засновані на стійкості дискретного логарифма в групі точок ЕК.

Кожна з цих схем може бути детермінована або рандомована. Застосування детермінованих схем характеризується тим, що цифровий

підпис одним і тим же вхідним рядком даних, приводить до формування однакових цифрових підписів. У рандомованій схемі при генерації підпису використовується деякий випадковий параметр, що приводить до формування різних підписів, навіть для однакових вхідних рядків. У рандомізованих схемах необхідно забезпечити непередбачуваність випадкових чисел [15; 32].

У свою чергу детерміновані схеми діляться на схеми ЕЦП одноразового застосування і схеми ЕЦП багаторазового застосування. Розглянемо основні стандарти ЕЦП, застосованих у комплексних системах захисту банківської інформації, проведемо зіставлення основних характеристик ЕЦП (довжину ключів, довжину цифрового підпису, складність (час) обчислення і складність (час) перевірки дійсності цифрового підпису) з метою виявлення їх переваг і недоліків, за умови, що рівень стійкості підпису стосовно будь-яких методів фальсифікації не нижче, ніж 10^{21} (або 30 років безперервної роботи мережі з 1000 суперкомп'ютерів).

У якості “базової” довжини ключів і довжини самого цифрового підпису будемо розглядати довжину в 64 байти.

Цифрові підписи з відновленням повідомлення є об'єктом розгляду двох стандартів ISO/IEC 9796 (1991 року) і ISO/IEC 9796-2 (1997 року). У стадії розробки перебуває четверта частина стандарту ISO/IEC 9796-4. Механізми ЕЦП певні в ISO/IEC 9796 застосовуються тільки до коротких повідомлень, тоді як механізми ISO/IEC 9796-2 застосовуються до повідомлень довільної довжини.

Стандарт ISO/IEC 14888 визначає механізми ЕЦП другого класу. Дані механізми застосовані до повідомлень довільної довжини. При обчисленні цифрових підписів з додаванням особливу роль відіграють однобічні хеш-функції. Хеш-функції також є об'єктом міжнародної стандартизації. Зокрема основним нормативним документом у даній області є міжнародний стандарт ISO/IEC 10118. Він складається з декількох частин і вводить модель хеш-функції (ISO/IEC 10118-1(1994 року), розглядає два методи для побудови хеш-функцій на основі блокових шифрів (ISO/IEC 10118-2 (1994 року), визначає три спеціалізованих (dedicated) хеш-функції, тобто хеш-функції, які розроблені спеціально для обчислення контрольних сум (ISO/IEC 10118-3 (1998 року).

Одна з них є стандартом NIST “Secure Hash Standard” (SHS). Дві інші RIPEMD-128 і RIPEMD-160 є розробкою Європейські організації зі стандартизації в рамках проекту “RIPE”. Нарешті ISO/IEC 10118-4 (1998 року) визначає дві хеш-функції на основі модульного зведення у

квадрат для використання з механізмами ЕЦП, що базуються на модульній арифметиці.

13.3.1.3. Механізми забезпечення управління доступом

Механізми управління доступом використовуються для забезпечення послуг управління доступом і реалізує політику управління доступом. При прийнятті рішень із приводу надання запитуваного типу доступу можуть використовуватися наступні види і джерела інформації:

- бази даних управління доступом, у яких можуть перебувати списки управління доступом або структури аналогічного призначення;
- паролі або інша ідентифікаційна інформація;
- токени, квитки або інші посвідчення, пред'явлення яких свідчить про наявність прав доступу;
- мітки безпеки, асоційовані із суб'єктами й об'єктами доступу;
- час запитуваного доступу;
- маршрут запитуваного доступу;
- тривалість запитуваного доступу та інша інформація.

Основні положення управління доступом відбиті в стандарті ISO/IEC 10181-3.

Механізми цілісності даних. Існує два типи механізмів забезпечення цілісності даних: механізми, спрямовані на захист цілісності окремого пакета даних, і механізми, спрямовані на забезпечення захисту цілісності послідовності пакетів даних.

Цілісність окремого пакета даних може бути забезпечена шляхом додавання до нього деякої контрольної величини, що є функцією від даних, що втримуються в пакеті. У ролі таких величин можуть виступати MAC-коди або криптографічні контрольні суми. Такі механізми можуть використовуватися для забезпечення як автентифікації джерела даних, так і для захисту цілісності даних і часто є інтегрованою частиною механізмів автентифікації й управління ключами. Однак даний механізм сам по собі не захищає від дублювання повідомлень. Механізми даного типу є об'єктом стандарту ISO/IEC 9797 (1994 року), що стандартизує механізми цілісності даних на основі використання блокового шифру в режимі зчеплення блоків. Цей стандарт опирається на більш ранні банківські стандарти, а саме на міжнародний стандарт ISO 8731-1 (1987 року) і банківські стандарти США ANSI X9.9 і X9.19 [32].

Механізми другого типу, які звичайно застосовуються разом з механізмами першого типу, можуть використовуватися для забезпечення послуг цілісності при організації зв'язку в режимі з встановленням з'єднання. Тут використовуються такі прийоми, як нумерація пакетів, часові штампи, криптографічне зв'язування та ін. Ці механізми дозволяють забезпечити захист від крадіжки, дублювання й вставки повідомлень. У мережах, що функціонують в режимі без встановлення з'єднання, використання часових штампів забезпечує також і обмежену форму захисту від дублювання.

Механізми автентифікації. В загальному випадку під автентифікацією розуміється встановлення дійсності повідомлення, джерела даних і приймача даних.

Автентифікація джерела даних часто забезпечується шляхом використання механізму захисту цілісності даних разом із шифруванням, або цифрового підпису. Логічна автентифікація користувача комп'ютерної системи здійснюється на основі пароля.

Автентифікація об'єкта комунікації звичайно виконується за допомогою подвійного або потрійного підтвердження з'єднання або "рукостискання", аналогічно процедурі синхронізації пакетів у протоколах із встановленням з'єднання.

Однобічний (однократний) обмін забезпечує тільки однократну автентифікацію і не може гарантувати своєчасність обміну. Двосторонній (двократний) обмін забезпечує взаємну автентифікацію джерела і приймача, але не забезпечує своєчасність обміну без застосування спеціальних засобів синхронізації. Тресторонній (трикратний) обмін дозволяє досягти повної взаємної автентифікації систем без додаткової синхронізації. Тут також для забезпечення автентифікації можуть використовуватися спеціальні механізми управління криптографічними ключами.

Механізми автентифікації, які ще відомі як протоколи автентифікації, є об'єктом різних стандартів. Міжнародний стандарт ISO/IEC 9798 визначає ряд таких механізмів, заснованих на різних криптографічних методах.

Стандарт складається з п'яти частин:

- ISO/IEC 9798-1 (1997 року) (друга редакція) містить загальну модель автентифікації об'єкта;
- ISO/IEC 9798-2 (1994 року) визначає механізми автентифікації на основі симетричного шифрування;

- ISO/IEC 9798-3 (1998 року) (друга редакція) визначає механізми автентифікації на основі ЕЦП;
- ISO/IEC 9798-4 (1995 року) визначає механізми автентифікації, засновані на використанні криптографічних хеш-функцій (на механізмах цілісності);
- ISO/IEC 9798-5 (1998 року) визначає механізми автентифікації, засновані на методах з “нульовими знаннями”.

Варіанти одно-, дво- або тристороннього обміну для автентифікації джерела даних розглядаються в стандарті розподіленої служби директорій X.500.

Двофакторна автентифікація або *2FA* – це метод ідентифікації користувача в будь-якому сервісі, де використовуються два різних типи автентифікаційних даних. Введення додаткового рівня безпеки забезпечує більш ефективний захист аккаунта від несанкціонованого доступу. Застосовуючи такий тип *2FA*, користувач вводить на першому рівні автентифікації персональний пароль. На наступному етапі він повинен ввести маркер *OTP* (*OTP* – *One-time Password Algorithm*), зазвичай відправлений за допомогою *SMS* на його мобільний пристрій. *OTP* буде доступний тільки тому, хто, як передбачається в теорії, ввів недоступний сторонньому пароль [39; 40]. Методи строгої (двофакторної) автентифікації найчастіше використовуються в фінансовій сфері, але в принципі можуть застосовуватися практично в будь-якій іншій області. Загальна класифікація методів багатфакторної автентифікації наведена на рис. 13.19.

Виділяють декілька основних способів побудови систем двофакторної автентифікації:

1. *ПЗ для ідентифікації конкретного ПК*. В комп’ютер встановлюється спеціальна програма, що використовує в ньому криптографічний маркер. Тоді в процесі автентифікації будуть задіяні два фактори: пароль і маркер, вбудований в ПК. Оскільки маркер постійно знаходиться на даному комп’ютері, користувачеві для входу в систему потрібно лише ввести ім’я користувача та пароль.

2. *Біометрія*. Використання біометрії як вторинного фактора ідентифікації здійснюється шляхом ідентифікації фізичних характеристик людини (відбиток пальця, оболонка очей тощо).

3. *Одноразовий e-mail або sms-пароль*. Використання як вторинного фактору ідентифікації *OTP*-пароля можливо шляхом відправлення другого

одноразового пароля на зареєстрований адресу електронної пошти або на мобільний телефон.

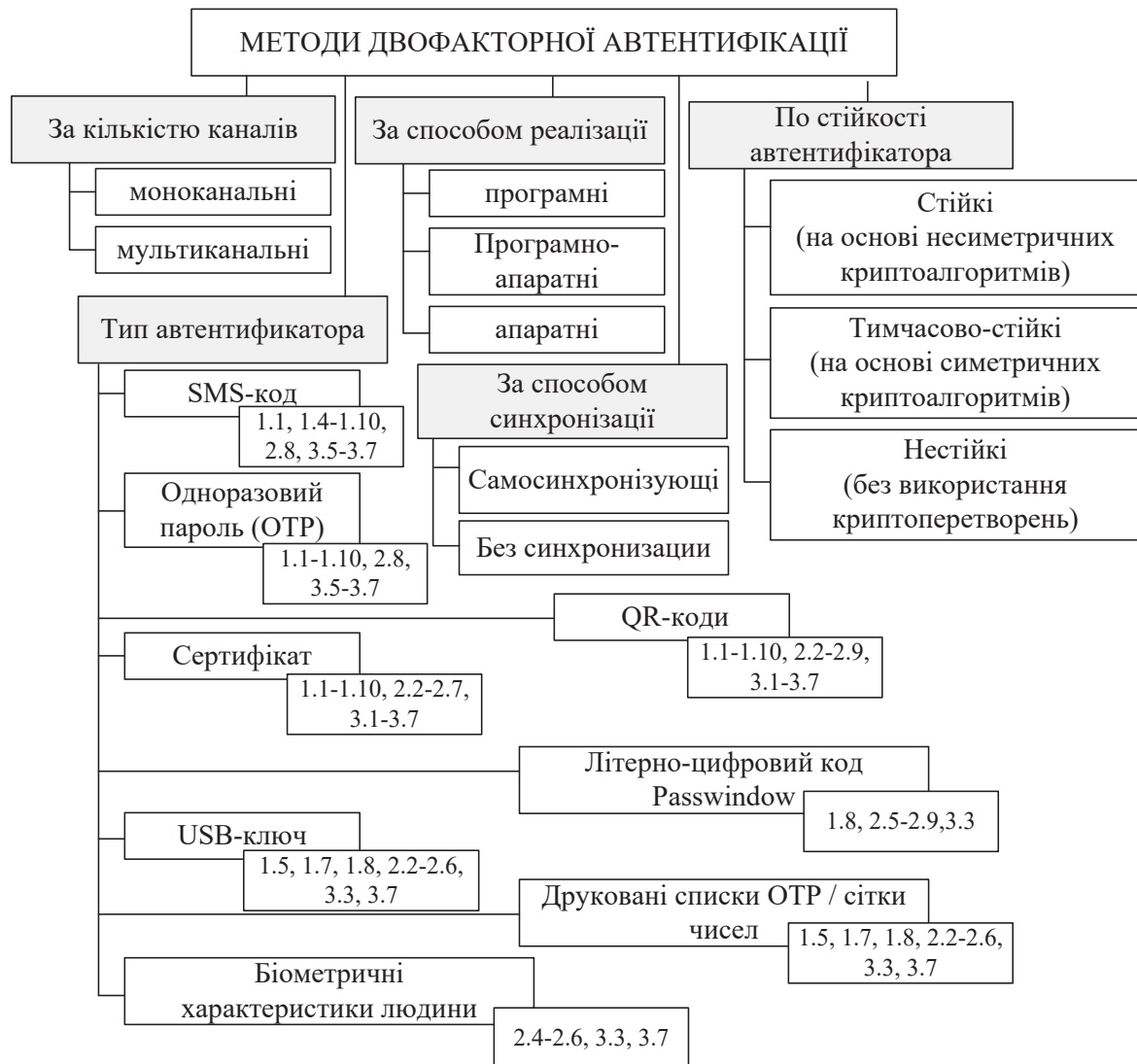


Рисунок 3.19. Класифікація методів багатофакторної автентифікації

4. *Токен з одноразовим паролем.* Користувачеві видається пристрій, який генерує постійно змінювані паролі. Саме ці паролі і вводяться користувачем додатково до звичайних паролів при автентифікації.

5. *Контроль зовні.* Цей метод передбачає дзвінок з банку на попередньо зареєстрований телефонний номер. Користувач повинен ввести пароль по телефону, і тільки після цього він отримає доступ до системи.

6. *Ідентифікація з використанням гаджетів.* Такого роду ідентифікація здійснюється шляхом приміщення криптографічної мітки на який-небудь пристрій користувача (наприклад, встановлені на USB-

накопичувач, *iPad*, карту пам'яті тощо.). При реєстрації користувач повинен під'єднати цей пристрій до ПК.

7. *Картка з шаром, що зішкрібається.* Користувачеві видається картка з *PIN*-кодом, який використовується лише один раз.

Аналіз методів багатофакторної автентифікації виявив основні переваги та недоліки систем *2FA*:

Методи на основі SMS-сповіщення. Їх перевагою є генерація *OTP*-кодів при кожному вході і передача по додатковому каналу. Перехоплення логіна і пароля користувача за основним каналом не приведуть зловмисника до банківської інформації клієнта. Недоліками прив'язки *OTP*-пароля до телефонного номеру клієнта є те, що використання відкритого каналу стільникового зв'язку не дозволяє забезпечити конфіденційність *OTP*-кодів, використання тільки стільникових каналів призводить до “втрати” двофакторної автентифікації. Існує теоретична ймовірність підміни номера через послугу оператора або працівників салонів зв'язку.

Використання методів з додатками-автентифікатора (QR-коди) дозволяє підтримувати кілька акаунтів в одному автентифікаторі і формувати первинний ключ, немає необхідності використовувати стільникові лінії зв'язку, генерація *OTP*-паролів на основі криптоалгоритмів. Основними недоліками є використання автентифікатора на тому ж пристрої, з якого здійснюється вхід призводить до “втрати” двофакторності, доступ зловмисника до первинного ключа користувача призводить до злому системи автентифікації.

Перевірка входу за допомогою мобільних додатків дозволяє автоматизувати процес автентифікації без участі користувача на основі перевірки особистого ключа автентифікації на мобільному додатку. Основними недоліками є: втрата / розкриття особистого ключа призводить до злому системи автентифікації, можливість отримання *SMS*-повідомлень за рахунок синхронізації між *iPhone* і *Mac*, використання автентифікатора на тому ж пристрої, з якого здійснюється вхід, призводить до “втрати” багатофакторності.

Фізичні (або апаратні) токени є найбільш надійним способом двофакторної автентифікації. Найчастіше вони представлені у вигляді *USB*-брелків з власним процесором, що генерує криптографічні ключі, які автоматично вводяться при підключенні до комп'ютера. Перевагами є відсутність використання додаткових мобільних додатків, ПЗ, токени є повністю незалежними девайсами. До *недоліків* належить те, що використання

декількох акаунтів призводить до 'зв'язки токенів, що не підтримується всіма застосунками.

Резервні ключі, є запасним варіантом на випадок втрати / крадіжки смартфона, на який приходять одноразові паролі або коди підтвердження. Втрата / крадіжка резервних ключів призводить до руйнування конфіденційності системи автентифікації.

Штрих-коди системи Passwindow забезпечують унікальні статичні зображення послідовності символів, що генеруються динамічно сервером автентифікації без використання криптоалгоритмів. Будь-яке втручання або підробка шаблону штрих-коду буде пасивно представлене користувачеві у вигляді появи комбінацій в шаблоні, який не відповідає сподіванням. Істотним *недоліком* є можливість підбору унікального штрих-коду картки.

Використання біометрії як вторинного фактора ідентифікації здійснюється шляхом ідентифікації фізичних характеристик людини (відбиток пальця, райдужна оболонка ока і т.п.). *Перевагами методів* є використання унікальних фізіологічних характеристик людини, відсутність додаткових мобільних додатків і ПЗ. Істотним *недоліком* є специфічні вимоги до програмно-апаратних пристроїв зчитування біометричних даних користувача. Таким чином, в автоматизованих банківських системах, як правило, застосовуються системи багатофакторної автентифікації, засновані на одноразових *e-mail* або *sms-паролях* і різних типах токенів. Для забезпечення конфіденційності в стандарті дистанційного банкінгу для передачі банком *ОТР-кодів* необхідно використовувати шифрований і незалежний від операторів канал їх доставки. Такий підхід не піддається впливу більшості відомих загроз, крім соціальної інженерії, що експлуатує людський фактор.

Механізми заповнення трафіку. Механізм заповнення трафіку застосовується для забезпечення конфіденційності трафіку. Заповнення трафіку може включати генерацію випадкового трафіку, заповнення додатковою інформацією інформативних пакетів, передачу пакетів через проміжні станції в "непотрібному" напрямку. Обидва типи пакетів – як інформативний, так і випадковий можуть доповнюватися до постійної довжини.

Механізми заповнення трафіку ефективні тільки в сполученні із засобами забезпечення конфіденційності, оскільки в протилежному випадку противнику буде очевидний фіктивний характер додаткових повідомлень.

Механізми нотаризації (арбітражу, завірення). Механізми нотаризації залучають третю сторону, що користується довірою двох суб'єктів, для

забезпечення підтвердження комунікаційних характеристик переданих даних. Такими комунікаційними характеристиками є цілісність, час, особистості відправників і одержувачів. Найчастіше механізми нотаризації застосовуються для забезпечення послуги підтвердження причетності. Для підтвердження причетності відправника даних нотаризація застосовується разом із цифровим підписом на основі “відкритого” ключа.

Нотаризація може також застосовуватися для забезпечення надійної часової мітки, забезпечуваної “часовим нотаріусом”. Така мітка може містити підпис “нотаріуса”, ідентифікатор повідомлення, ім’я відправника і одержувача, а також зареєстровані час і дату одержання повідомлення. При цьому “нотаріус” не має доступу до самого повідомлення, ніж дотримується конфіденційність повідомлення.

Механізми нотаризації є об’єктом стандарту ISO/IEC 13888, що містить три частини:

- ISO/IEC 13888-1 (1997 року) описує загальну модель непричетності;
- ISO/IEC 13888-2 (1998 року) визначає механізми непричетності, засновані на криптографічних контрольних сумах (наприклад MAC-коди);
- ISO/IEC 13888-3 (1997 року) визначає, яким чином в інтересах нотаризації можуть використовуватися цифрові підписи.

Механізми управління маршрутизацією застосовуються для забезпечення конфіденційності з метою запобігання контролю за шляхом проходження даних від відправника до одержувача. Вибір шляху може здійснюватися або кінцевою системою, реалізуючи маршрутизацію, обумовлену джерелом (source routing), або проміжною системою на основі використання “міток безпеки”, що вводяться в пакет кінцевою системою. Цей механізм вимагає забезпечення надійності (довірчості) проміжних систем і може мати істотні варіації при використанні різних систем. Він може також використовуватися й для забезпечення захисту цілісності даних (з функціями відновлення даних або з’єднання) за рахунок введення і використання для передачі даних альтернативних шляхів у випадку виникнення атак, що приводять до переривання комунікацій.

У такий спосіб механізми управління маршрутизацією спрямовані на вирішення таких завдань:

- забезпечення конфіденційності;
- вибір тільки фізично надійних каналів і проміжних систем при передачі даних;
- заборона передачі даних ненадійними каналами;

– вибір альтернативних шляхів проходження даних при виявленні постійних атак (загроз) на шляху проходження.

13.3.2. Загальні механізми забезпечення безпеки

У стандарті ISO 7498-2 визначені наступні загальні механізми забезпечення безпеки [58]: довірча функціональність (trusted functionality), мітки безпеки (security lables), виявлення подій (event detection), контроль безпеки (security audit trail), відновлення безпеки (security recovery).

Довірча функціональність використовується разом з іншими механізмами безпеки і становить сукупність рекомендацій і способів, які повинні бути реалізовані для забезпечення гарантії правильної і надійної роботи інших механізмів безпеки. Довірча функціональність допускає широке використання нормативної документації при розробці програмних або апаратних засобів, що реалізують механізми безпеки. Розробка цих засобів повинна вестися при дотриманні відповідних організаційних вимог. Програмні та апаратні засоби повинні розроблятися, тестуватися і сертифікуватися на основі єдиних методик. Тут же забезпечуються всі необхідні вимоги і рекомендації до електромагнітних випромінювань, можливостей фізичного втручання, з використання безпечних каналів поширення та ін.

Мітки безпеки. Будь-який ресурс (записані дані, обчислювальні потужності і/або комунікаційні послуги) може мати асоційовані з ними мітки безпеки, які позначають їх рівень таємності. Мітки безпеки можуть бути явно або побічно зв'язані як окремими пакетами даних, так і з послідовностями пакетів. Звичайно мітки безпеки використовуються для реалізації методики управління доступом на основі встановлених правил, а також для управління маршрутизацією.

Передані дані також можуть мати мітки безпеки, які передаються разом з ними безпечним чином. У цьому випадку для забезпечення захисту міток застосовуються криптографічні функції, а мітки безпеки використовуються для забезпечення контролю за цілісністю повідомлень.

Виявлення подій. Механізми виявлення подій у системах захисту інформації служать для виявлення як спроб порушення безпеки, так і для реєстрації легітимної активності користувачів. Виявлення може бути локальним і/або дистанційним і реалізується через тривожну сигналізацію про події (event reporting (alarm)), реєстрацію подій (event logging) і

відбудовні дії (recovery actions). Реалізація механізмів виявлення спроб порушень безпеки – досить складне завдання, що вимагає залучення методів штучного інтелекту. Тут проблема полягає у визначенні того мінімуму інформації, який би дозволив виявити (або не пропустити) можливі події з втручання в роботу комп'ютерної системи.

Реєстрація контролю безпеки. Під контролем безпеки розуміють незалежний розгляд і аналіз записів безпеки з метою перевірки достатності управління системою, гарантувати відповідність функціонування системи політиці безпеки і рекомендувати необхідні зміни в управлінні, політиці і процесах безпеки. Звичайно розглядають дві процедури: протоколювання і аудит.

Під протоколюванням розуміється збір і нагромадження інформації про події, що відбуваються в інформаційній системі.

Під аудитом розуміється оперативний аналіз накопиченої інформації, проведений постійно або періодично.

Механізми протоколювання і аудиту служать для рішення наступних задач:

- забезпечення підзвітності користувачів і адміністраторів, що є засобом стримування;
- забезпечення можливості відновлення послідовності подій, що дозволяє виявити слабкі місця в захисті інформації, виявити винуватця вторгнення, оцінити масштаби заподіяного збитку і повернутися до нормальної роботи;
- надання інформації для виявлення та аналізу проблем, через підготовку відповідних звітів і рапортів.

Особливістю протоколювання й аудиту є їх залежність від послуг і механізмів безпеки. Так, ідентифікація і автентифікація служать відправною точкою підзвітності користувачів. Для забезпечення конфіденційності та цілісності реєстраційної інформації застосовують механізми управління доступом. Можливе застосування й криптографічні засоби. Основною проблемою при реалізації механізмів протоколювання і аудиту є формулювання критеріїв відбору записів, що бідують у детальному аналізі.

Відновлення безпеки. Механізми відновлення безпеки виконують функцію реакції системи на порушення безпеки. Такими діями можуть бути, наприклад, негайне роз'єднання або припинення роботи, відмова суб'єкта в

доступі, тимчасове позбавлення суб'єкта прав, занесення суб'єкта в “чорний список” і т. д.

13.3.3. Взаємозв'язок послуг та механізмів безпеки і взаємозв'язок послуг і рівнів моделі BBC

Одним з компонентів стандарту ISO 7498-2 є співвіднесення послуг безпеки і механізмів безпеки [58].

Табл. 13.2 показує, які механізми (окремо або в комбінації з іншими) можуть використовуватися для реалізації тієї або іншої послуги безпеки.

Стандарт також співвідносить послуги забезпечення безпеки з рівневою EMBC.

У табл. 13.2 зазначені рівні еталонної семирівневої моделі BBC, на яких можуть бути реалізовані функції безпеки. Розглянемо більш докладно застосування послуг безпеки на різних рівнях EMBC.

Фізичний рівень. Послуги забезпечення безпеки, запропоновані на Фізичному рівні, забезпечують захист каналів, організованих за схемою “точка – точка”, наприклад, між двома кінцевими системами або між кінцевою і проміжною системами. Дія цієї послуги закінчується в точці закінчення каналу перед пристроєм прийому або комутації пакетів.

Засоби і пристрої, що забезпечують безпеку на цьому рівні, звичайно прив'язані до конкретної технології передачі сигналів і інтегровані з фізичним інтерфейсом, що приводить до необхідності використовувати ідентичні пристрої на обох кінцях фізичного або віртуального з'єднання. Як видно з табл. 13.2, застосування засобів захисту на фізичному рівні обмежується послугами забезпечення конфіденційності для комунікацій із встановленням з'єднання і захисту трафіку. Іншим обмеженням використання засобів захисту на фізичному рівні є складність управління ними.

Біт-орієнтований інтерфейс фізичного рівня не дозволяє реалізувати послуги автентифікації та цілісності даних через неможливість виконувати перетворення даних. Однак використання підходящої техніки шифрування на цьому рівні може створити гарну базу для використання послуг забезпечення безпеки на більш високих рівнях.

Канальний рівень. Послуги забезпечення безпеки каналного рівня реалізуються для з'єднань типу “точка – точка” аналогічно до послуг фізичного рівня. Перевагою застосування послуг забезпечення безпеки на цьому рівні є їх незалежність від протоколів більш високого рівня. Однак тут

теж існує сильна залежність практичної реалізації від використовуваної технології фізичного рівня. Відповідно до рекомендацій ISO 7498-2 послуги, запропоновані на цьому рівні, включають конфіденційність для систем із встановленням і без встановлення з'єднання.

Таблиця 13.2

Розподіл функцій безпеки за рівнями ЕМВС

Послуги безпеки	Рівні моделі BBC						
	1	2	3	4	5	6	7
Автентифікація об'єкта			Так	Так			Так
Автентифікація джерела даних			Так	Так			Так
Управління доступом			Так	Так			Так
Конфіденційність з'єднання	Так	Так	Так	Так			Так
Конфіденційність без встановлення з'єднання		Так	Так	Так			Так
Конфіденційність виділеного поля даних							Так
Конфіденційність трафіку	Так		Так				Так
Цілісність з'єднання з відновленням				Так			Так
Цілісність з'єднання без відновлення			Так	Так			Так
Цілісність виділеного поля в режимі із встановленням з'єднання							Так
Цілісність виділеного поля в режимі без встановлення з'єднання							Так
Цілісність блоку даних без з'єднання			Так	Так			Так
Причетність до посилки повідомлення							Так
Підтвердження одержання повідомлень							Так

Мережний рівень. Безпека на мережному рівні забезпечується між кінцевими системами незалежно від проміжних міжмережних комутаторів і мостів рівня подання даних. Якщо послуги забезпечення безпеки ґрунтуються повністю на протоколах мережного рівня, то це забезпечує безпека комунікацій між кінцевими системами уздовж різнорідних мереж, що формують, наприклад, Інтернет. Стандарт ISO 7498-2 рекомендує застосування декількох послуг забезпечення безпеки на мережному рівні: конфіденційності (для систем із встановленням і без встановлення з'єднання, для захисту від контролю трафіку), управління доступом, захисту цілісності

даних у системах із встановленням і без встановлення з'єднання, а також автентифікації джерела даних і об'єкта комунікацій.

Відповідно до рекомендацій ISO 7498-2 послуги забезпечення безпеки повинні бути сумісні з відповідними комунікаційними послугами на кожному рівні і, по можливості, їх використовувати, що часто приводить до залежності реалізованих послуг забезпечення безпеки від протоколів мережного рівня або унеможливорює їх застосування [58].

Послуги забезпечення безпеки, що повністю використовують протоколи мережного рівня, тобто реалізовані “поверх” мережного рівня, можуть забезпечувати захищеність комунікацій у багатопрокольних мережах. При цьому послуги забезпечення безпеки можуть бути реалізовані у міжмережних (або проміжних) системах або пристроях. Це дає ряд переваг, пов'язаних з тим, що міжмережні пристрої часто служать шлюзами або портами між різними локальними і глобальними мережами. Реалізація послуг забезпечення безпеки і захищеності в таких прикордонних пристроях ефективна з погляду необхідності мінімальної модернізації існуючих систем. Додаткові засоби безпеки можуть бути розміщені між міжмережними пристроями і кінцевими системами при використанні тих же протоколів і послуг.

Незалежна реалізація послуг забезпечення безпеки на мережному рівні дозволяє застосовувати ці послуги тільки відносно таких об'єктів, як мережі, що є досить “трубим” підходом. Для окремих груп мережних протоколів існують можливості забезпечити вибірковість таких послуг, ґрунтуючись на адресації протоколів більш високого рівня в протоколах мережного рівня, як це зроблено в протоколах TCP/IP з адресацією вищих протоколів і портів у пакетах мережного і транспортного рівнів. Однак це порушує принцип рівневості і у загальному випадку не застосовується.

Додаткова можливість для забезпечення вибірковості послуг забезпечення безпеки на мережному рівні може бути реалізована через параметр “якість послуги”, обумовлений кінцевою системою та оброблюваний проміжними системами. Зокрема стандарт захищеного протоколу мережного рівня NLSP допускає таку можливість.

Включення послуг забезпечення безпеки мережного рівня до складу функцій кінцевої системи, як правило, вимагає модифікації ядра операційної системи, тому що більшість мережних ОС включають функції мережного рівня у своє ядро з метою досягнення великої продуктивності і безпеки системи.

Транспортний рівень. На транспортному рівні стандарт ISO 7498-2 визначає набір послуг забезпечення безпеки, дуже близький за складом до набору послуг мережного рівня: конфіденційність (для систем із встановленням і без встановлення з'єднання), контроль за доступом, захист цілісності в системах із встановленням і без встановлення з'єднання, автентифікацію джерела даних і об'єкта комунікації. Відмінністю є те, що послуги забезпечення безпеки транспортного рівня реалізуються тільки в кінцевих системах, на відміну від можливості реалізації послуг на базі мережного рівня в проміжних системах.

Реалізація послуг транспортного рівня із встановленням з'єднання в загальному випадку забезпечує більш високу захищеність комунікацій порівняно з реалізацією таких же послуг на більш високих рівнях з використанням протоколів і послуг більш низького рівня. Але при правильному використанні комунікаційних можливостей транспортного рівня такі відмінності можуть бути несуттєвими. Так само, як і для мережного рівня, багато механізмів забезпечення безпеки транспортного рівня інтегровані до складу мережних ОС і визначаються їх розроблювачами.

Сеансовий рівень і рівень подання даних. ISO 7498-2 не рекомендує застосування послуг забезпечення безпеки на сеансовому рівні і рівні подання даних. Це викликано тим, що ці рівні не мають певних комунікаційних послуг і функцій. Застосування багатьох послуг на основі шифрування на рівні подання даних недоцільна через те, що функції цього рівня зазвичай інтегровані до складу прикладного рівня.

Прикладний рівень. Стандарт ISO 7498-2 дозволяє застосування всіх послуг забезпечення безпеки на прикладному рівні, а застосування послуги причетності рекомендується тільки на цьому рівні. Однак використання послуг забезпечення безпеки тільки на прикладному рівні не дозволяє повністю захистити системи комунікацій від всіх можливих атак, тому рекомендується одночасно забезпечувати підтримку конкретних послуг також і на більш низьких рівнях. При цьому очевидно, що додатки типу обміну повідомленнями або служби директорій можуть бути реалізовані тільки на прикладному рівні [58].

Найбільш привабливою рисою застосування послуг забезпечення безпеки на прикладному рівні є їх незалежність від ОС і можливість реалізувати ці послуги в складі додатків, але при цьому використовувані механізми стають специфічними для конкретного додатка.

13.3.4. Управління безпекою

Під *управлінням безпекою* (security management) розуміють управління і поширення інформації, необхідної для роботи функцій і механізмів безпеки, а також збір і аналіз інформації про їх роботу та спроби порушення безпеки. Прикладами управління безпекою можуть служити поширення криптографічних ключів, установка значень параметрів захисту, ведення реєстраційного журналу і т. д.

Концептуальною основою управління безпекою є інформаційна база управління безпекою (ІБУБ) (Security Management Information Base), що є інтегрованою частиною інформаційної бази управління (ІБУ) (Management Information Base). ІБУБ може містити в собі таблиці даних, файли, дані й правила, вбудовані в апаратні або програмні засоби. Ця база може не існувати як єдине розподілене сховище, але кожна з кінцевих систем зобов'язана мати інформацію, необхідну для впровадження в життя обраної політики безпеки.

Стандарт ISO 7498-2 визначає чотири ієрархічних рівні управління безпекою [58]: управління системою безпеки в цілому, управління послугами безпеки, управління механізмами безпеки, забезпечення безпеки управління ЕМВС.

Управління системою безпеки в цілому містить у собі управління політикою безпеки, взаємодію з іншими службами управління ВВС, реагування на події, що відбуваються, аудиту й безпечне відновлення, підтримку методики управління доступом.

Управління послугами безпеки містить у собі визначення об'єктів, що захищаються, вироблення правил (критеріїв) вибору механізмів безпеки для реалізації необхідних послуг, комбінування механізмів безпеки, взаємодії з іншими адміністраторами для забезпечення погодженої роботи.

Управління механізмами безпеки здійснює управління окремими механізмами безпеки. Типовий список таких механізмів містить у собі:

1. *Управління ключами.* Це фундамент будь-якого механізму безпеки, заснованого на використанні криптографічних засобів. Управління ключами містить у собі безпечну генерацію, розподіл, зберігання, відновлення, видалення і знищення криптографічних ключів. Багато аспектів управління ключами виходять за межі середовища ВВС. У наш час розроблений міжнародний стандарт управління ключами – ISO/IEC 11770, що опирається на відповідні банківські стандарти, зокрема на ISO 11166.

2. *Управління шифруванням* має на увазі установку і синхронізацію криптографічних параметрів. До управління шифруванням можна віднести і управління механізмами цифрового підпису, а також управління цілісністю, якщо вона забезпечується криптографічними засобами.

3. *Адміністрування управління доступом* містить у собі розподіл інформації управління доступом.

4. *Управління автентифікацією*, тобто розподіл інформації, необхідної для автентифікації – паролів, ключів і т. п.

5. *Управління доповненням трафіку* має на увазі вироблення й підтримку правил, що задають характеристики узагальнень, що доповнюють, – частоту відправлення, розмір і т. п.

6. *Управління маршрутизацією* виражається у виділенні надійних шляхів.

7. *Управління нотаризацією*, тобто поширення інформації про нотаріальні служби і адміністрування цих служб.

Нарешті безпека управління охоплює функції управління, що забезпечують безпеку керуючих повідомлень.

Безпека управління включає захист ІБУ і забезпечення безпеки зв'язку між частинами розподіленої ІБУ.

Взаємозв'язок функцій і механізмів безпеки наведено на рис. 13.20.

13.4. Основні принципи захисту інформації при підключенні до мережі Інтернет

Для підключення мережі організації (будь-який) до мережі Інтернет необхідно прийняти ряд певних організаційно-технічних заходів для її захисту.

При побудові захисту варто виходити з того, що будь-який захист ускладнює використання системи, що, за прямим призначенням обмежує функціональні можливості, споживає обчислювальні й трудові ресурси, вимагає фінансових витрат на створення та експлуатацію. Чим вище захист, тим дорожчою у побудові та обслуговуванні стає система і тим менш зручною для безпосередніх користувачів [1; 6 – 8; 13; 15 – 17; 22 – 24; 26 – 32; 34; 35; 41 – 45].

Тому захищаючи мережу варто виходити з доцільної вартості захисту. Тобто витрати на захист повинні бути пропорційні цінності ресурсу, що

захищає. Існує ряд основних принципів, що дозволяють організувати досить безпечне підключення до Internet порівняно простими засобами.

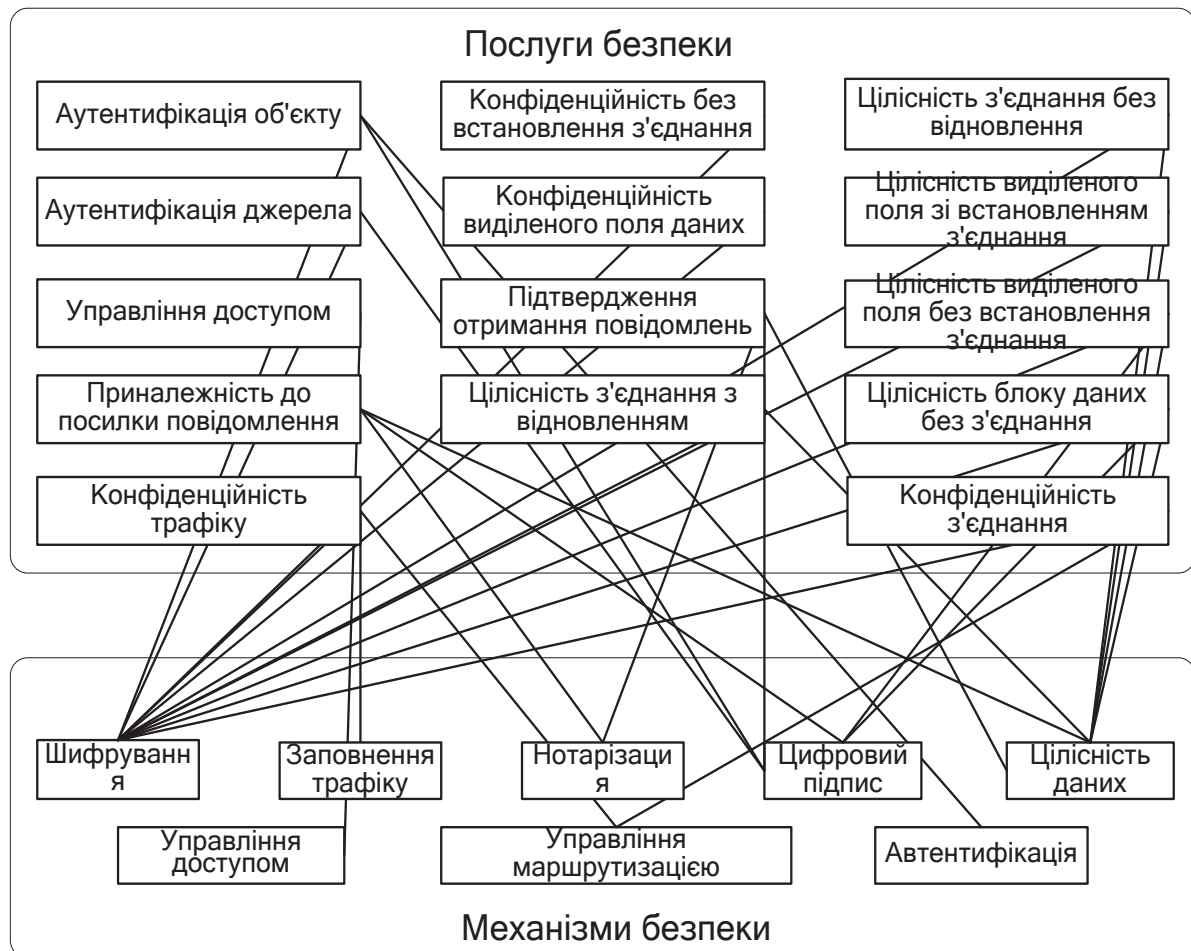


Рис. 13.20. Функції і механізми безпеки

Firewall (Брандмауер)

Основним загальновизнаним засобом такого захисту є міжмережний екран (Брандмауер) [16; 41].

Міжмережний екран встановлюється між мережею та Internet і виконує роль мережного фільтра (рис. 13.21).

Він настраюється таким чином, щоб пропускати допустимий трафік від користувачів мережі до служб Internet і назад, і обмежити трафік з боку Internet до мережі, яка потребує захисту, тільки необхідними службами, наприклад: smtp, dns, ntp.

Допустимість того або іншого трафіка визначається мережним адміністратором відповідно до політики інформаційної безпеки організації. (Наприклад, може бути дозволений доступ із частини комп'ютерів мережі до

web та ftp-серверів Internet і двонаправлений доступ між Internet та поштовим сервером, але при цьому заборонені всі інші протоколи й напрямки трафіка).

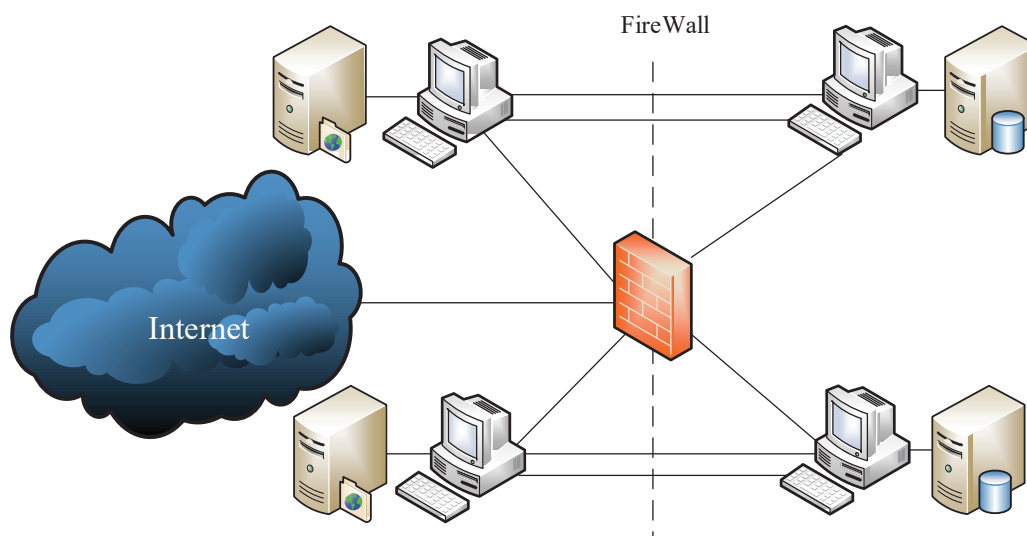


Рис. 13.21. Встановлення брандмауера у локальній мережі

Таким чином, міжмережний екран фізично розташовується на місці мережного шлюзу (маршрутизатора), логічно представляється доцільним сполучити їх функції в одному пристрої. Це дозволяє одним засобом захистити й локальну мережу і безпосередньо сам шлюз. Така опція передбачена для маршрутизаторів компанії Cisco Systems (Firewall Feature Set). Однак дане правило є необов'язковим і міжмережний екран може бути поданий окремим пристроєм.

У найпростішому випадку виконання функцій міжмережного екрана можна організувати за допомогою мережного фільтра на основі аркушів доступу (access-lists). Аркуші доступу визначають правила, за якими або дозволяється, або забороняється проходження трафіка з певними ознаками від одного мережного інтерфейсу маршрутизатора до іншого усередині самого маршрутизатора. Як ознаки можуть використовуватися IP-адреси або діапазон, IP-адреса джерела й приймача, тип протоколу, номер порту призначення або відправлення, ряд інших службових ознак IP-пакета.

Відмінність і недолік аркушів доступу порівняно із сьогоdnішнім міжмережним екраном полягає у тому, що вони дозволяють створити статичний одnobічний фільтр, тоді як мережне з'єднання становить динамічний процес. Аркуші доступу не дозволяють контролювати параметри IP-пакета, що залежать від попередніх пакетів. Звідси виникає складність

застосування аркушів доступу для тонкого настроювання фільтрації трафіка в точній відповідності із прийнятою політикою безпеки. Зокрема, із цієї причини аркуші доступу не в змозі захистити від такого різновиду мережної атаки, як “викрадення з’єднання”, або “хай-джекінг”.

У Firewall Feature Set зазначені проблеми вирішуються за допомогою того, що він відслідковує кожне мережне з’єднання окремо і контролює весь процес у динаміку. При встановленні нового TCP-сеансу міжмережний екран створює для нього новий процес, що контролює правильність з’єднання до самого моменту його завершення. При цьому кожний пакет на транспортному рівні перевіряється на відповідність попередній, а всі “підозрілі” пакети відбраковуються. Завдяки цьому стає можливим досить легко організувати фільтр для доступу внутрішнього комп’ютера до зовнішнього, але не дозволяє зовнішньому комп’ютеру самостійно звернутися до внутрішнього.

Іншими словами, у настроюваннях міжмережного екрана задаються правила для проходження трафіка від одного інтерфейсу до іншого, для кожного напрямку й кожного тракту окремо. Якщо правило дозволяє проходження IP-пакета від інтерфейсу внутрішньої мережі до Internet-інтерфейсу, то на підставі такого пакета формується логічний тунель у маршрутизаторі, через який уже можуть пройти відповідні пакети від зовнішнього одержувача. Як тільки з’єднання закрито, або вичерпаний час очікування, тунель закривається, і обіг ззовні до внутрішнього комп’ютера буде відкинутий. З цієї ж причини екран не пропустить пакети у зворотному напрямку, якщо ініціатором з’єднання є зовнішній комп’ютер.

Крім того, міжмережний екран, на відміну від аркушів доступу, може контролювати зміст IP-пакетів у полі даних і відбраковувати пакети, що містять потенційно-небезпечні коди, наприклад, java-апліти. Є міжмережні екрани, здатні виявити в IP-пакетах ознаки відомих мережних атак і перервати таке з’єднання, але це вже досить дорогі системи.

З найбільш дешевих систем слід зазначити Firewall на основі ядра операційної системи Linux версії 2.4.20 і вище й засоби керування iptables. Через те що Linux є безкоштовною ОС, витрати на побудову такого міжмережного екрана зводяться до придбання звичайного персонального комп’ютера із двома мережними інтерфейсами. Проте Linux дозволяє побудувати досить надійний і гнучкий мережний фільтр, що розпізнає окремі прапори в службових полях IP-пакета.

NAT

Другою цеглинкою забезпечення захищеності мережі є “заміна мережної адреси” – Network Address Translation, або NAT. Вона становить заміну в IP-пакеті реальної адреси комп’ютера внутрішньої мережі на будь-яку іншу задану адресу при посиланні його в зовнішню мережу. Завдяки цьому для внутрішньої мережі стає можливим використання діапазонів адрес, які не застосовуються в Internet (наприклад, 10.0.0.0 – 10.255.255.255). Це дозволяє запобігти прямому обігу ззовні до внутрішніх комп’ютерів і приховує структуру мережі. Існує кілька різновидів NAT [9–12].

Найпростіша й найбільш марна з погляду захисту – це трансляція фіксованої внутрішньої адреси у фіксовану зовнішню. При цьому противник безперешкодно “бачить” такий комп’ютер у зовнішній мережі, тому що йому однозначно відповідає певна зовнішня адреса. Однак вона необхідна при організації сервера, до якого потрібно забезпечити доступ ззовні (рис. 13.22).

Друга форма NAT – це трансляція групи внутрішніх адрес в одну зовнішню. При цьому всі внутрішні комп’ютери можуть працювати з Internet одночасно, а маршрутизатор розрізняє, кому яка відповідь перетрансльовується за службовими даними TCP-з’єднання. У зовнішній мережі створюється враження, що до неї звертається тільки один комп’ютер. Така заміна істотно ускладнює життя противнику, тому що повністю приховує внутрішні комп’ютери й перешкоджає “обчисленню” жертви (рис. 13.23).

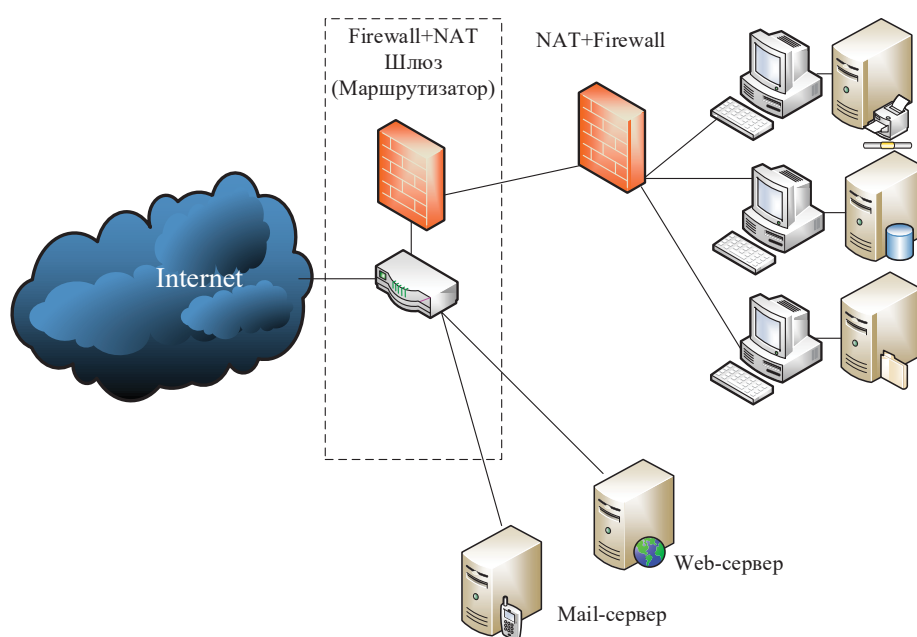


Рис. 13.22. Трансляція фіксованої внутрішньої адреси у фіксовану зовнішню

Зловмисник, навіть бачучи трафік, що виходить із внутрішньої мережі, не може визначити, від якого комп'ютера він виходить. Крім того, це виключає можливість ініціативного обігу ззовні до внутрішнього комп'ютера, тому що для маршрутизатора в цьому випадку відсутнє правило прив'язки зовнішньої адреси до внутрішньої. Зокрема виключається можливість сканування ззовні внутрішньої мережі.

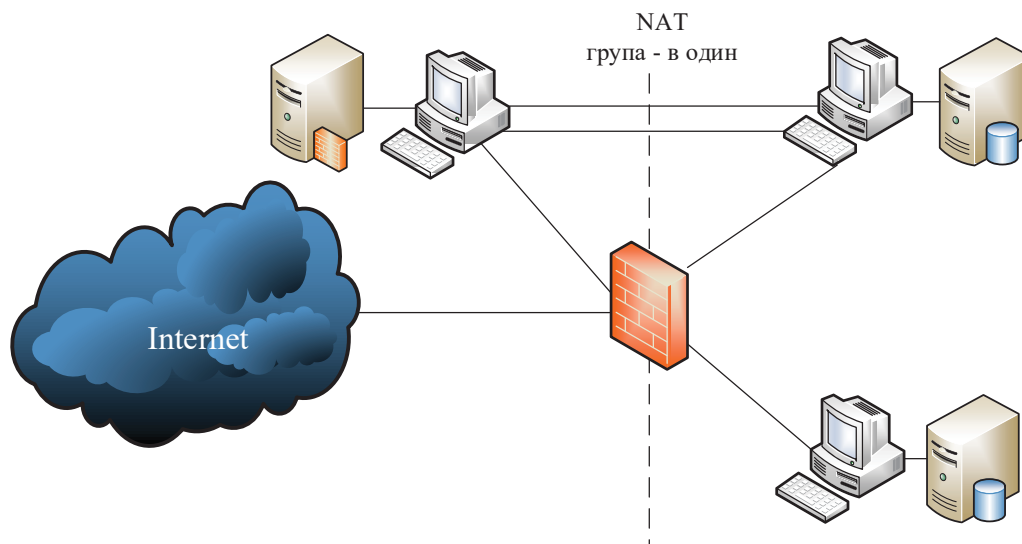


Рис. 13.23. Трансляція групи внутрішніх адрес в одну зовнішню

Третя форма NAT – використання для заміни внутрішніх адрес не однієї адреси, а будь-якої з виділених адрес. Тобто, внутрішній комп'ютер, виходячи в Internet, одержує вільну у цей момент адресу з бази даних (БД). При цьому адреси підмінюються динамічно, і кожне нове TCP-з'єднання може бути встановлене з іншою IP-адресою. Це також створює додаткові труднощі противнику, тому що позбавляє його можливості атакувати будь-який внутрішній комп'ютер прицільно. Сказане відносно другої форми NAT є справедливим і для третьої форми. Якщо запит приходить ззовні, то маршрутизатор не в змозі зв'язати адресу з БД з адресою мережі. Тому такий запит не досягне мети.

Демілітаризована зона

Як правило, організації потрібно мати у себе деякі мережні ресурси, до яких відкритий доступ з Internet. Звичайно це поштовий, dns і web-сервери [9–12,]. Механізм їх роботи допускає, що до них повинен бути дозволений вільний або слабко обмежений обіг з Internet. Відповідно ймовірність їх зламу

вища, ніж інших комп'ютерів мережі. Із цієї причини розміщати їх усередині зони, яка захищається, недоцільно з погляду безпеки, тому що у випадку зламу вони можуть стати воротами для атаки внутрішніх комп'ютерів. Для мінімізації ризику і збереження функціональності такі сервери встановлюють за основним шлюзом мережі, але перед міжмережним екраном, що забезпечує захист внутрішніх комп'ютерів. Логічну область їх розміщення називають демілітаризованою зоною (рис.13.24).

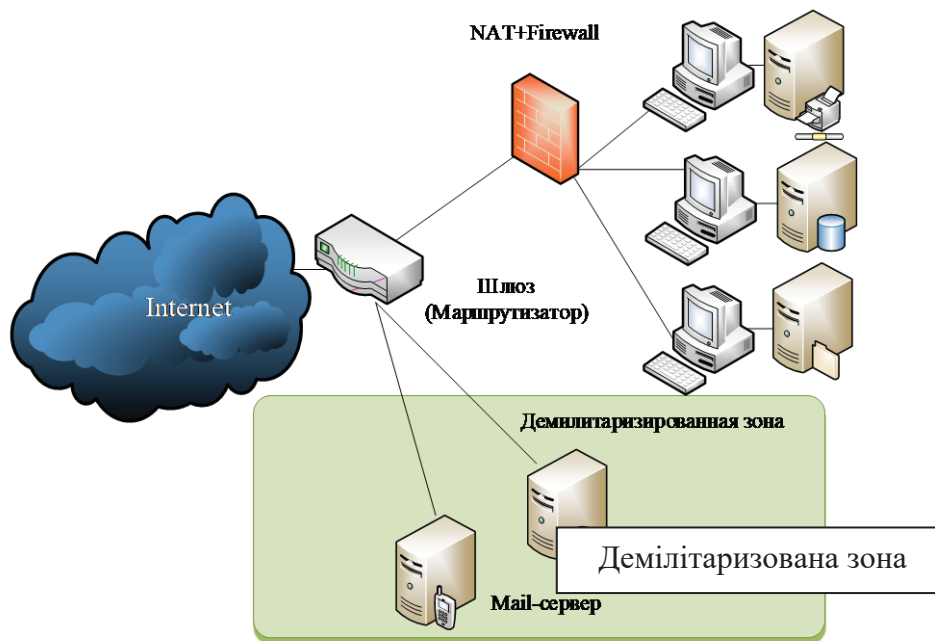


Рис. 13.24. Демілітаризована зона

Другий firewall

З рис. 13.24 видно, що ніщо не заважає встановити другий Firewall на основному шлюзі мережі. Це є логічним рішенням і дозволяє одночасно підвищити рівень захисту внутрішньої мережі й захистити сервери демілітаризованої зони. При правильному налаштуванні обох міжмережних екранів противнику буде вже набагато сутужніше дістатися до внутрішньої мережі організації. Наявність другого міжмережного екрана ускладнює конфігурування мережного встаткування й налаштування роботи всіх елементів мережі. Для додаткового підвищення захищеності можна використати Firewall-и різних виробників. Тоді якщо в одному з них буде виявлена вразливість, інший не дозволить противнику безперешкодно проникнути у мережу, як це мало б місце при використанні Firewall-ів одного типу [16; 17; 24].

Особливо варто підкреслити, що можливість мережного доступу до шлюзів і до міжмережних екранів, щоб уникнути зловмисного використання,

повинна бути відключена. З погляду безпеки пристрої, які знаходяться на стражі мережі, повинні конфігуруватися й заадмініструватися тільки через консольний порт локально (рис. 13.25).

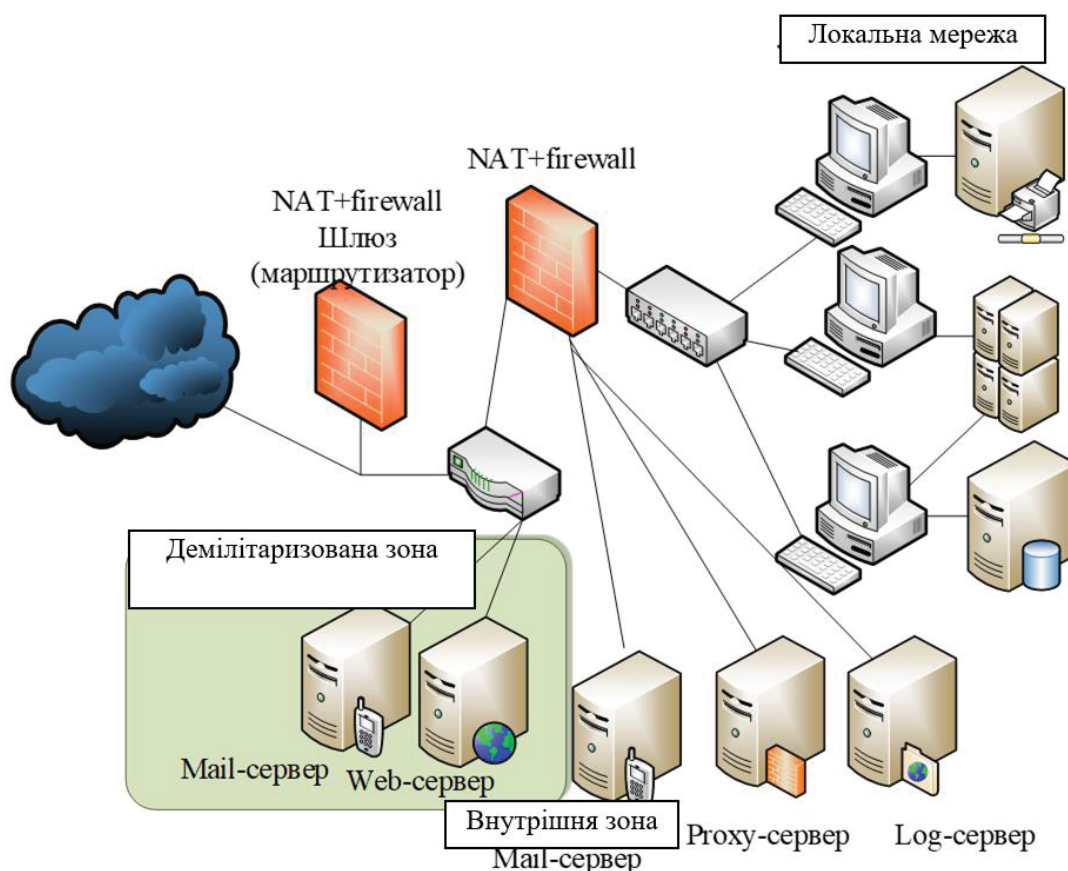


Рис. 13.25. Локально-консольний порт для серверів

Схема, запропонована на рис. 13.25, може бути дещо вдосконалена. Для цього необхідно використати граничний маршрутизатор із двома Ethernet-портами.

Proху-сервер

Використання так званого “посередника” (проху-сервера) також підвищує рівень захищеності мережі, тому що виключає необхідність прямого виходу в Internet комп’ютерів користувачів [16; 17; 24; 41]. При цьому також стає можливим більш строгий контроль за даними в IP-пакетах на рівні мережних додатків. Proху-сервер працює як посередник між користувацьким додатком і вилученим мережним ресурсом в Internet. Схематично сутність його роботи показана на рис. 13.26.

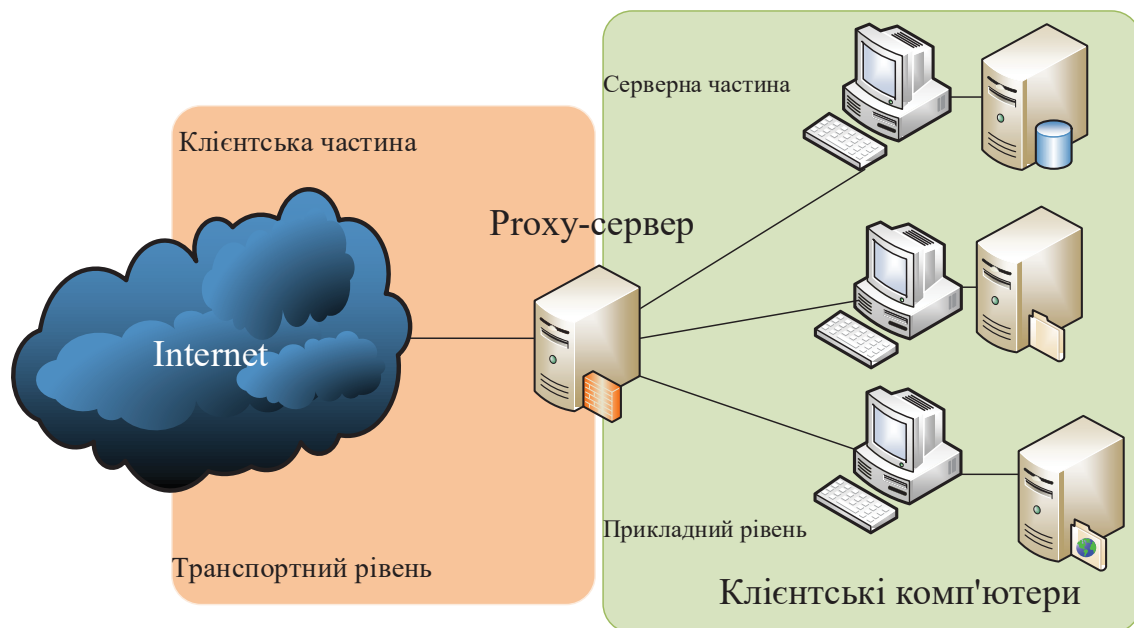


Рис. 13.26. Proxy-сервер

Проксі-сервер складається ніби із двох частин, клієнтської і серверної. Клієнтська частина дивиться у сторону Internet, серверна – у сторону клієнтського комп'ютера. Коли клієнтський комп'ютер звертається до вилученого сайту через проксі-сервер, його клієнтський мережний додаток взаємодіє із серверною частиною проксі-сервера. При цьому проксі-сервер на рівні додатка передає клієнтський запит своєї клієнтської частини, і вона вже від імені проксі-сервера надсилає даний запит на вилучений сайт. Тобто IP-пакет що відправлений має адресу проксі-сервера.

Потім отримана відповідь передається у зворотну сторону від клієнтської частини проксі-сервера його серверної частини, з якою безпосередньо взаємодіє користувальницький комп'ютер. Таким чином, пряме з'єднання клієнтських комп'ютерів з вилученим сайтом виключається. Усередині проксі-сервера передача даних між клієнтською частиною й серверною відбувається вже не на транспортному рівні, а на рівні протоколу додатка, ніж забезпечується легкість контролю команд і даних на відповідність установленим стандартам. Крім того, це дозволяє забезпечити досить надійний контроль проти передачі зловмисних кодів усередині даних. Навіть у випадку успішної атаки з боку Internet за відкритими протоколами у цьому випадку буде ушкоджений тільки проксі-сервер, що не представляє інформаційної цінності, а користувальницькі комп'ютери будуть залишатися в безпеці ще якийсь час.

Через те що проху-сервер працює тільки за декількома відомими протоколами (HTTP, FTP та інших) і не пропускає через себе інші пакети, він сильно обмежує можливості противника з використання мережних “троянських коней” для закріплення на будь-якому з користувальницьких комп’ютерів.

Другий mail-сервер

Залишати mail-сервер у демілітаризованій зоні з однієї сторони небажано, тому що на ньому фактично зберігається поштова база даних з перепискою локальних користувачів, а демілітаризована зона не може забезпечити належного рівня захисту мережним ресурсам. З іншого боку, якщо сховати mail-сервер усередині локальної мережі, то він або не зможе взаємодіяти із зовнішнім середовищем, або буде становити ворота із зовнішнього середовища у внутрішню локальну мережу, якими потенційно зможе скористатися противник [16; 17; 24; 41].

Внаслідок цього доречним рішенням є використання двох поштових серверів. Основний сервер устатковується усередині мережі, яка захищена, і його не видно для зовнішнього світу. Всі локальні користувачі поштової системи заводяться на нього і мають до нього прямий доступ. Відповідно вся вхідна кореспонденція зберігається на ньому у поштових скриньках локальних користувачів. Відправлення електронної пошти також здійснюється через нього.

Другий, або зовнішній, поштовий сервер устатковується в демілітаризованій зоні й забезпечує взаємодію по e-mail з Internet. Він настраюється таким чином, щоб всю пошту, що приходить на ім’я користувачів організації, відразу пересилати на внутрішній поштовий сервер. У такий спосіб у його поштової бази даних немає ні одного облікового запису користувачів організації і жоден аркуш не відкладається для довгострокового зберігання. Тому якщо він виявиться зламанним зломисником, то противник не одержить доступу до накопиченої переписки. Проте після зламу противник одержує можливість перехоплення й читання транзитної пошти. Тому потрібен ретельний контроль за подібною ситуацією й негайне вживання заходів при підозрі на НСД (несанкційного доступу).

Перевагою такої схеми є те, що навіть зі зламаного зовнішнього поштового сервера не так просто дістатися до внутрішньої захищеної мережі. Обмін даними між зовнішніми й внутрішніми поштовими серверами відбувається через міжмережний екран з єдиним дозволеним портом (SMTP) за єдиною дозволеною парою адрес. Звертання до інших комп’ютерів і по

інших протоколах буде блокуватися. Тому впливати з нього прямо на комп'ютери користувачів внутрішньої мережі неможливо.

Антивірусний захист поштової системи

Операційна система Windows дуже вразлива перед деякими різновидами поштових вірусів. Користувачу буває досить встановити покажчик на інфікований конверт, щоб вірус активізувався. Але більш небезпечним є те, що механізм роботи поштових вірусів може бути використаний зловмисником для закидання в область мережного “троянського коня”, якими захищається. Він дозволить противнику таємно скачувати дані з вашої мережі та здобути всю інформацію, що цікавить. Тому забезпеченню антивірусного захисту тракту доставки пошти у внутрішню мережу варто приділити досить серйозну увагу [13; 17; 26; 35; 42–45].

Існує ряд програмних засобів, призначених для контролю кореспонденції на поштових серверах на предмет наявності в ній вірусів у процесі прийому й пересилання електронної пошти.

Принцип її роботи полягає в тому, що вся пошта, що проходить через сервер, спочатку перенаправляється спеціальному користувачу, у ролі якого виступає антивірусний процес. Він сканує зміст кожного аркуша на наявність у ньому фрагментів відомих вірусів. Якщо аркуш містить щось схоже на вірус, воно вилучається із процесу передачі й, залежно від налаштувань антивірусу, піддається заданій обробці. Повідомлення про виявлений вірус відсилаються відправнику й одержувачу інфікованого аркушу, а також на ім'я зазначених адміністраторів системи. Після перевірки аркуші, що не викликають підозри, відсилаються за призначенням.

Тим самим на рівні поштового сервера ставиться надійний захист відомим вірусам у електронній пошті. Через те що антивірусна програма розпізнає тільки віруси, сигнатури яких перебувають у її базі даних, необхідно регулярно оновлювати антивірусну базу даних з офіційного сайту. Інакше мережа може стати уразливою для знову створених вірусів.

Log-сервер

Загальновідомий механізм протоколювання системних подій на серверах і клієнтських робочих станціях. Розроблювачі програмного забезпечення включають у свої продукти фрагменти коду, які на ту або іншу подію генерують відповідні текстові повідомлення, що посилають операційній системі. Система збирає дані повідомлення в log-файлах, які потім можуть аналізуватися адміністратором або користувачем з метою з'ясування, які події відбувалися в системі деякий час потому. Це дозволяє,

наприклад, з'ясувати, чому не запускається та або інша програма, або чому припинив функціонувати певний сервіс. Дуже корисні log-файли для пошуку слідів зламу системи й відвідування її несанкціонованими гостями. Через те що злом, як правило, супроводжується множиною заборонених дій, це породжує велику кількість системних повідомлень, що осідають в log-файлах [17; 41]. Із цієї причини противник завжди прагне стерти сліди своєї присутності, або видаливши log-файли, або їх підчистивши. В обох випадках адміністратору після цього буде важко зрозуміти, що ж відбулося в системі насправді – яким чином у неї проникнули, як довго в ній перебували, ніж встигли покористуватися. Або навіть просто переконатися, що все добре.

Тому обов'язковою умовою для мережі, підключеної до Internet, є наявність у ній окремого log-сервера.

Принцип його роботи полягає в тому, що кожна операційна система може посилати повідомлення про системні події за UDP-протоколом на вилучений сервер. Це можуть робити також маршрутизатори й міжмережні екрани. Збираючи такі повідомлення на спеціально виділеному сервері, ми забезпечуємо їм схоронність від рук противника. Тому для мінімізації ймовірності зламу log-сервер повинен бути призначений тільки для збору log-повідомлень. Він не повинен виконувати будь-яких інших функцій і виконувати інші мережні додатки, крім syslogd. У цьому випадку після зламу будь-яких комп'ютерів мережі на log-сервері залишаться відповідні повідомлення, знищити які противник уже не зможе.

Таким чином, у результаті найбільш оптимальної є наступна схема підключення локальної мережі до Internet (рис. 13.27).

Таким чином, проведений аналіз способів захисту комп'ютерних мереж при підключенні їх до глобальної мережі Інтернет показав, що для забезпечення захисту при обміні інформацією абоненти локальної мережі повинні використовувати принципи і засоби безпеки в комплексі з організаційними заходами. Це дозволить надійно захистити від атак як активних, так і пасивних противників.

13.4.1. Захист інформації за допомогою міжмережних екранів

Серед програмно-апаратних і програмних засобів забезпечення автентичності, розподілених КМ, можна виділити міжмережні екрани (ММЕ), засоби аналізу захищеності й засоби виявлення атак.

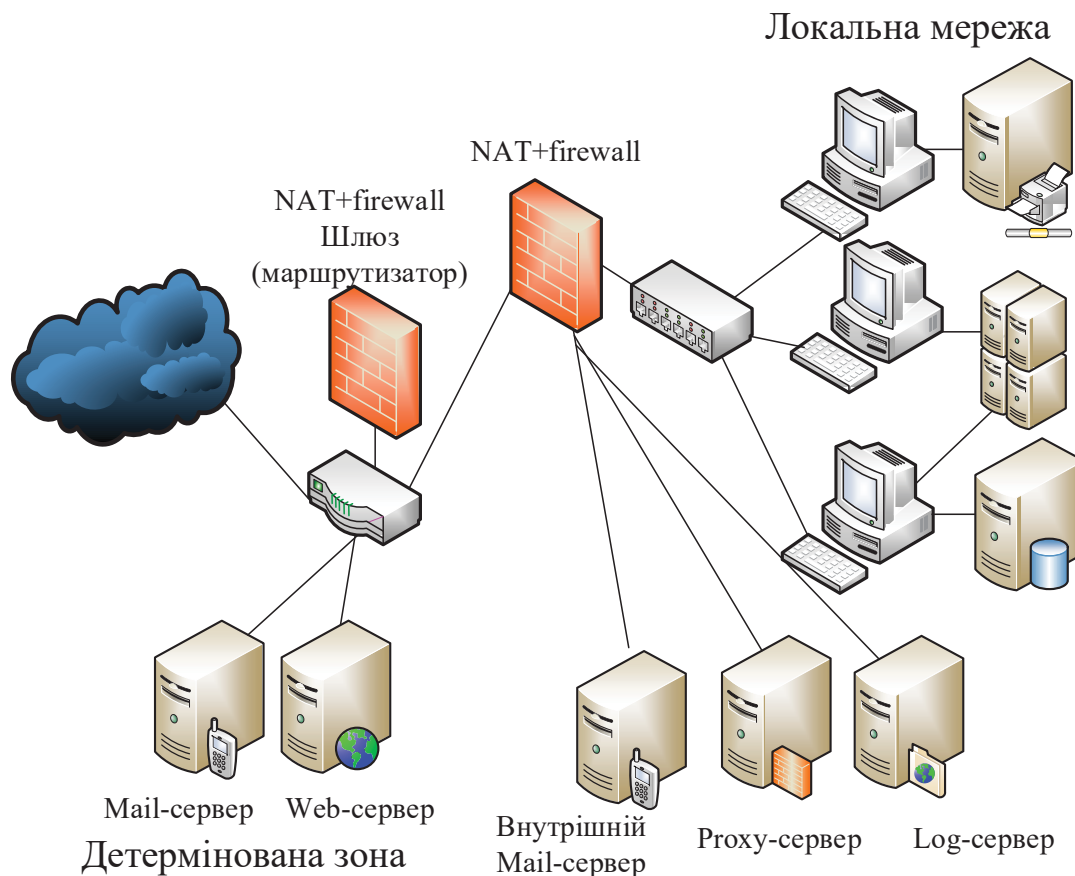


Рис. 13.27. Схема з Log-сервером

Міжмережні екрани (брандмауери, firewall) реалізують набір правил, які визначають умови проходження пакетів даних з однієї частини розподіленої КМ (відкритої) в іншу (захищену). Залежно від рівня взаємодії об'єктів мережі основними різновидами ММЕ є фільтруючі маршрутизатори, шлюзи сеансового й прикладного рівнів. Основною функцією фільтруючих маршрутизаторів, що працюють на мережному рівні еталонної моделі, є фільтрація пакетів даних, що входять у захищену частину мережі або вихідних з неї. Правила фільтрації визначають, дозволяється або блокується проходження через ММЕ пакета із правилами, що задаються цими параметрами.

До основних переваг фільтруючих маршрутизаторів відносяться простота їх створення, установка й конфігурування; прозорість для додатків користувачів КМ і мінімальний вплив на їх продуктивність; невисока вартість.

Недоліками фільтруючих маршрутизаторів є:

- відсутність автентифікації на рівні користувачів КМ;
- уразливість для підміни IP-адреси в заголовку пакета;

- незахищеність від погроз порушення конфіденційності й цілісності переданої інформації;
- сильна залежність ефективності набору правил фільтрації від рівня знань адміністратора ММЕ конкретних протоколів;
- відкритість IP-адрес комп'ютерів захищеної частини мережі.

Шлюзи сеансового рівня призначені для контролю віртуального з'єднання між робочою станцією захищеної частини мережі й хостом її незахищеної частини і трансляції IP-адрес комп'ютерів захищеної частини мережі.

У процесі виконуваного шлюзом сеансового рівня процедури трансляції IP-адрес відбувається їхнє перетворення в одну IP-адресу, асоційовану із ММЕ. Це виключає пряму взаємодію між хостами захищеної й відкритої мережі і не дозволяє порушнику здійснювати атаку шляхом підміни IP-адрес.

До переваг шлюзів сеансового рівня відносяться їх простота й надійність програмної реалізації. Недоліком є відсутність можливості перевіряти вміст переданої інформації. Це дозволяє порушнику намагатися передати пакети із шкідливим програмним кодом і звернутися потім прямо до одного із серверів, що атакується КМ.

Шлюзи прикладного рівня не тільки виключають пряму взаємодію між уповноваженим користувачем із захищеної частини мережі й хостом з її відкритої частини, але й фільтрують усі вхідні й вихідні пакети даних на прикладному рівні (на основі аналізу змісту переданих даних).

Основні функції шлюзів прикладного рівня:

- ідентифікація й автентифікація користувача КМ при спробі встановити з'єднання;
- перевірка цілісності переданих даних;
- розмежування доступу до ресурсів захищеної й відкритої частин розподіленої КМ;
- фільтрація і перетворення переданих повідомлень (виявлення шкідливого програмного коду, шифрування й розшифрування та ін.);
- реєстрація подій у спеціальному журналі;
- гешування запитуваних ззовні даних, розміщених на комп'ютерах внутрішньої мережі (для підвищення продуктивності КМ).

Перевагами шлюзів прикладного рівня також є:

- прихованість структури захищеної частини мережі для інших хостів;
- надійна автентифікація й реєстрація минаючих повідомлень;
- більш прості правила фільтрації пакетів на мережному рівні, відповідно до яких маршрутизатор повинен пропускати тільки трафік, призначений для шлюзу прикладного рівня, і блокувати весь інший трафік;
- можливість реалізації додаткових перевірок.

Основними недоліками шлюзів прикладного рівня є більш висока вартість, складність розробки, установки й конфігурування, зниження продуктивності КМ, “непрозорість” для додатків користувачів КМ.

Міжмережні екрани є основою для створення віртуальних приватних мереж (Virtual Private Network, VPN), які призначені для приховання топології внутрішніх мереж організацій, що обмінюються інформацією з мережею Інтернет, і захисту трафіка між ними. При цьому використовуються спеціальні системи маршрутизації.

Загальним недоліком ММЕ будь-якого виду є те, що ці програмно-апаратні засоби захисту в принципі не можуть запобігти багатьох видів атак (наприклад, погрози несанкціонованого доступу до інформації з використанням неправильного сервера служби доменних імен мережі Інтернет, погрози аналізу мережного трафіка, погрози відмови в обслуговуванні). Порушнику реалізувати погрозу доступності інформації в КМ, що використовує ММЕ, може виявитися навіть простіше, тому що досить атакувати тільки хост із ММЕ для фактичного відключення від зовнішньої мережі всіх комп’ютерів захищеної частини мережі.

13.4.2. Захист інформації на мережному рівні

13.4.2.1. Протокол IPSec

Протоколи мережевої безпеки IPSec (Internet Protocol Security (IPSec) – це стек протоколів, який працює на транспортному рівні та призначений для забезпечення цілісності, конфіденційності та автентичності інформаційних потоків [2, 62].

При цьому під конфіденційністю визначається спроможність забезпечити безпеку інформаційних потоків від пасивних атак у кіберпросторі.

Під цілісністю визначається здатність системи забезпечити безпеку при зберіганні, а також можливість модифікації тільки уповноваженим користувачем та/або процесом.

Під автентичністю визначається спроможність системи забезпечити підтвердження джерела інформації.

Основні протоколи IPsec [2, 62]:

- RFC2402 “IP Authentication Header” (AH), який забезпечує цілісність та автентичність інформаційних потоків у кіберпросторі;
- RFC2406 “IP Encapsulation Security Payload” (ESP), який на основі симетричних алгоритмів шифрування забезпечує конфіденційність інформаційних потоків у кіберпросторі;
- RFC2408 “Internet Security Association and Key Management Protocol” (ISAKMP), який на основі несиметричних криптосистем забезпечує перші два протоколи зміною ключових даних;
- RFC2409 “The Internet Key Exchange” (IKE), є подальшим розвитком і адаптацією ISAKMP, призначений для роботи з протоколами IPsec.

На рис. 13.29 наведена структурна схема стеку протоколів IPsec.

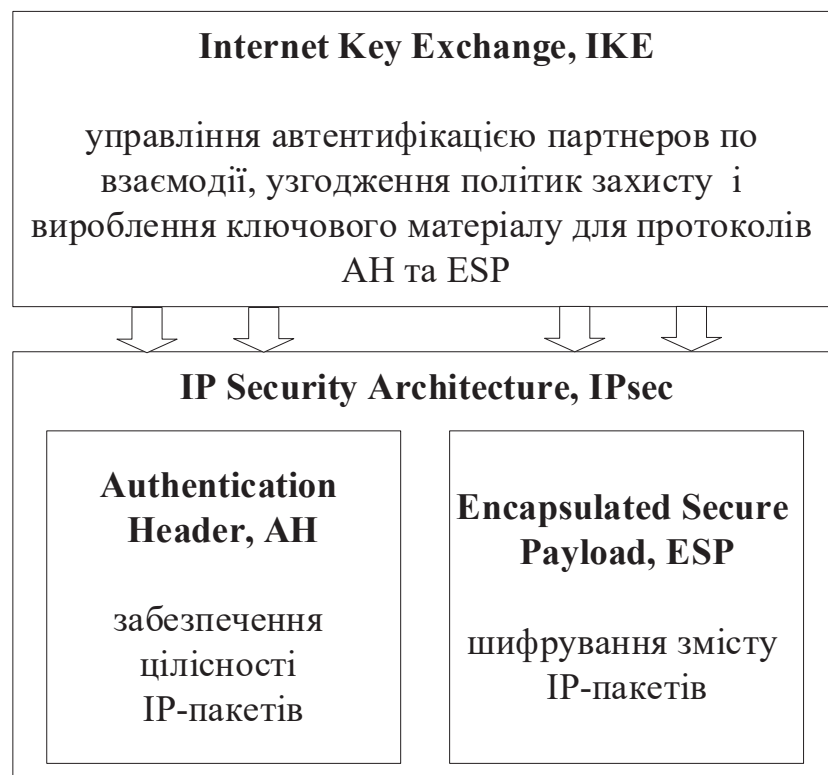


Рис. 13.29. Структурна схема протоколу IPsec

Для забезпечення конфіденційності інформаційних потоків у транспортному рівні використовуються блоково-симетричні шифри IDEA, CAST-128, 3DES, AES [2, 62], але їх криптостійкість в умовах появи повномасштабного квантового комп'ютера може не забезпечувати потрібний рівень безпеки.

Стек протоколів IPSec може використовувати транспортний або тунельний режим, структурні схеми яких наведені на рис. 13.30, 13.31 відповідно [2, 62].

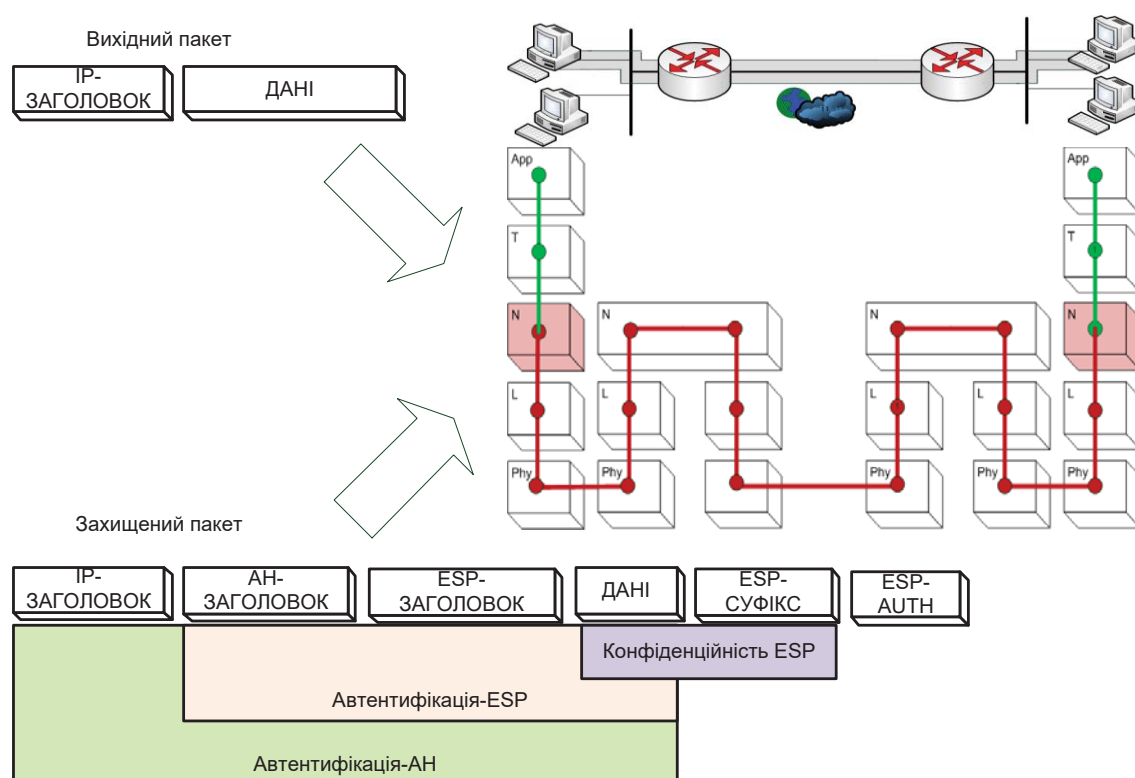


Рис. 13.30. Передача IP-пакету в транспортному режимі

У транспортному режимі забезпечується цілісність інформаційного потоку шляхом шифрування протоколом ESP, а також автентифікація внаслідок використання протоколу АН. При цьому забезпечується оперативність передачі інформаційного потоку. Однак поле з адресою отримувача передається у відкритому вигляді, що суттєво знижує рівень конфіденційності.

При використанні тунельного режиму забезпечуються такі послуги безпеки: за допомогою протоколу АН – автентичність інформаційного потоку, після чого весь пакет шифрується за допомогою симетричних

алгоритмів шифрування протоколу ESP, (рис. 13.31) [2, 62]. Однак при цьому необхідно забезпечити відсутність проміжних комутаційних пристроїв, тобто передача здійснюється за принципом “точка в точку”, що суттєво знижує можливість його використання в кіберпросторі.

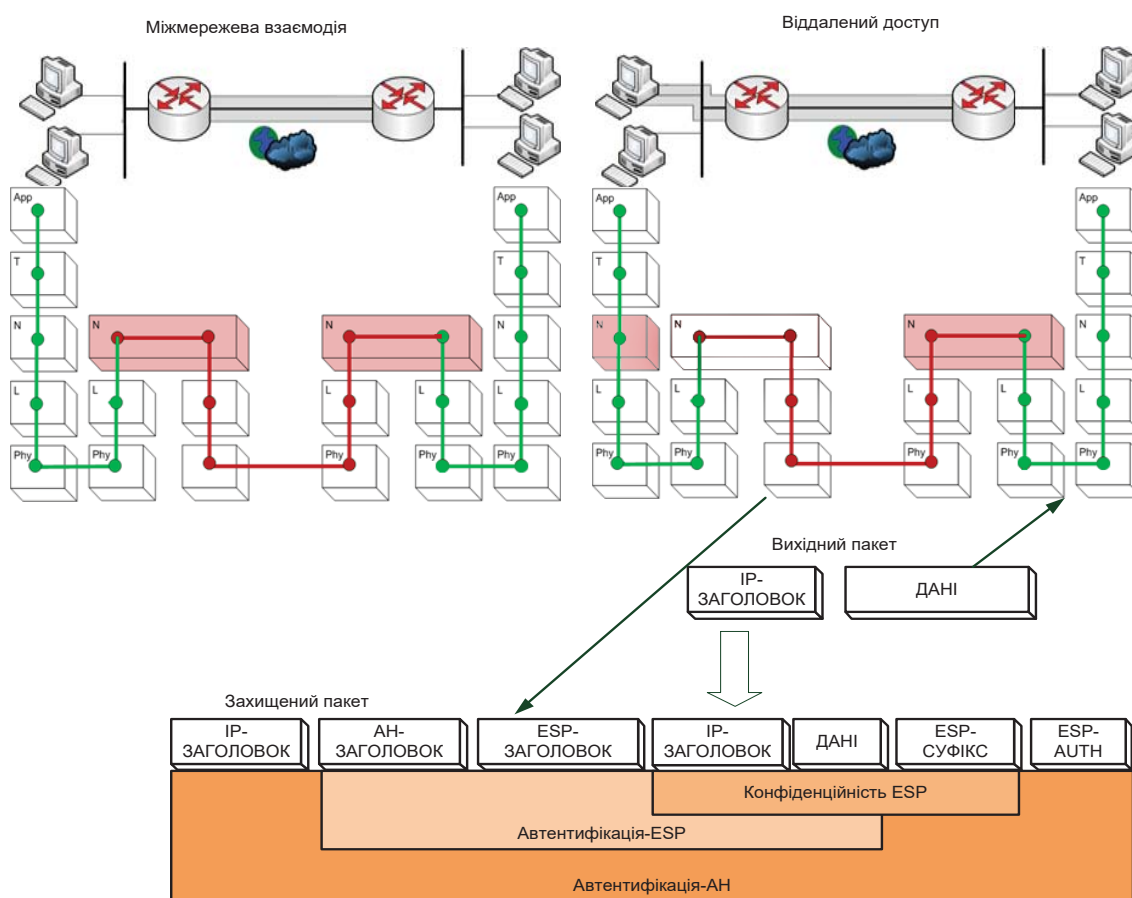


Рис. 13.31. Передача IP-пакета в тунельному режимі

Щоб цього уникнути необхідно використовувати додаткові шифратори на проміжних комутаційних пристроях, що значно підвищує енергетичні затрати, а також дозволяє зловмиснику при розшифруванні поля з адресою отримати необхідну інформацію [2, 62].

На сьогодні існує декілька практичних схем використання стека протоколу IPSec, в першу чергу це схема “хост-хост”, наведена на рис. 13.32. Як правило, цю схему використовують всередині корпоративної мережі для забезпечення конфіденційності передачі інформаційних потоків [2, 62]. Друга схема, яка наведена на рис. 13.33, забезпечує захищений канал між двома проміжними вузлами кіберпростору. Такий підхід забезпечує формування шлюзу безпеки.

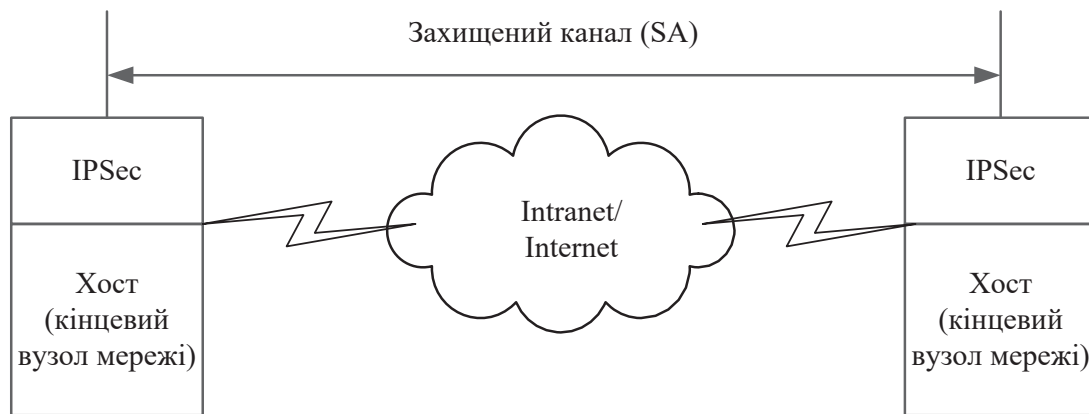


Рис. 13.32. Схема організації захищеного каналу “хост-хост”

При використанні другої схеми застосується тунельний режим, що значно знижує можливість його використання в кіберпросторі.

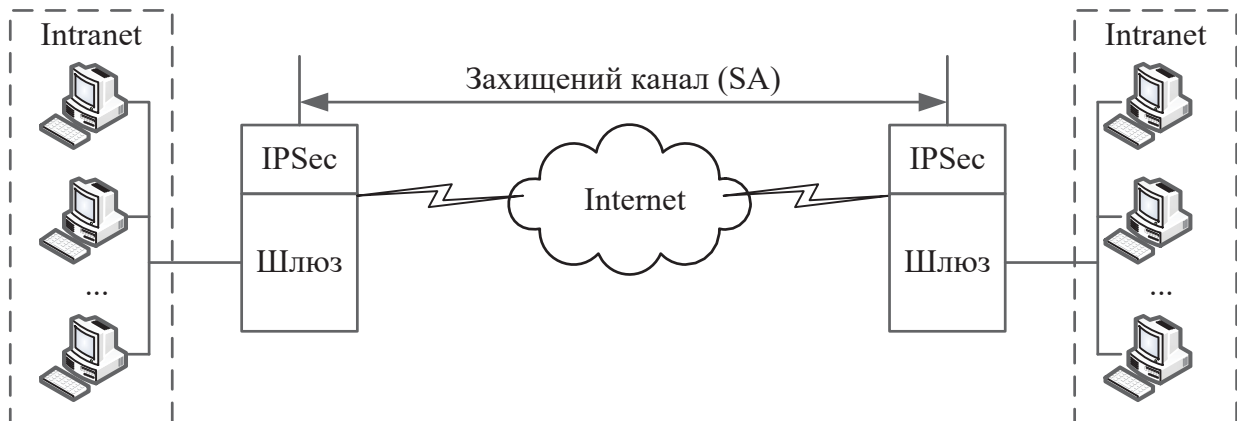


Рис. 13.33. Схема організації захищеного каналу “шлюз-шлюз”

Схема “хост-шлюз”, яка наведена на рис. 13.34, як правило, використовується при формуванні VPN-каналів [2, 48, 62], що дозволяє забезпечити конфіденційність та цілісність інформаційних потоків при віддаленому підключенні до корпоративної мережі хоста. При цьому, як правило, використовується тунельний режим, але може використовуватись і транспортний режим.

Для забезпечення цілісності та автентичності користувачів на транспортному рівні використовуються протоколи цілісності – SSL (Secure Socket Layer) або TLS (Transport Layer Security). Ці протоколи також забезпечують цілісність інформаційних потоків електронної пошти [2, 48, 62].

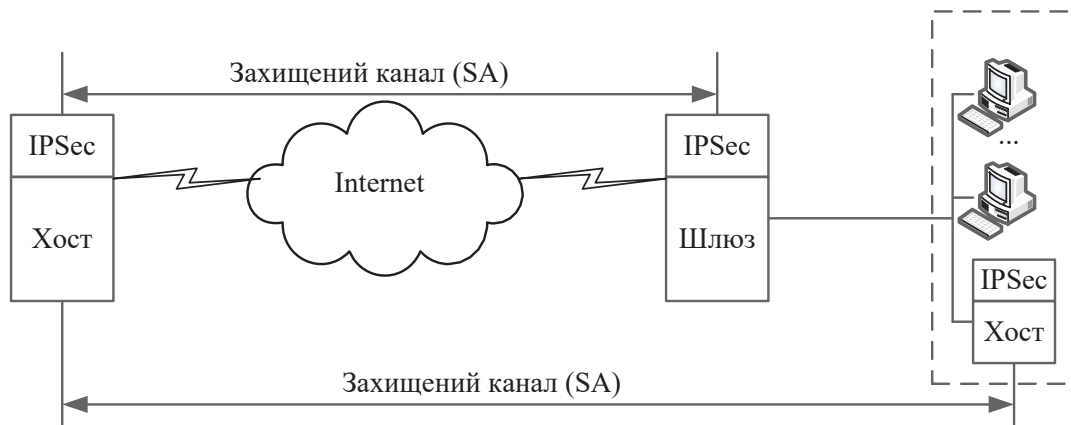


Рис. 13.34. Схема організації захищеного каналу “хост-шлюз” з додатковим каналом “хост-хост”

5.4.2.2. Протокол SSL

Протоколи SSL або TLS забезпечують цілісність інформаційних потоків за допомогою симетричних алгоритмів шифрування (3DES, AES), а також використовують MAC-коди для забезпечення послуги автентичності.

Структура протоколу SSL наведена на рис.13.35.

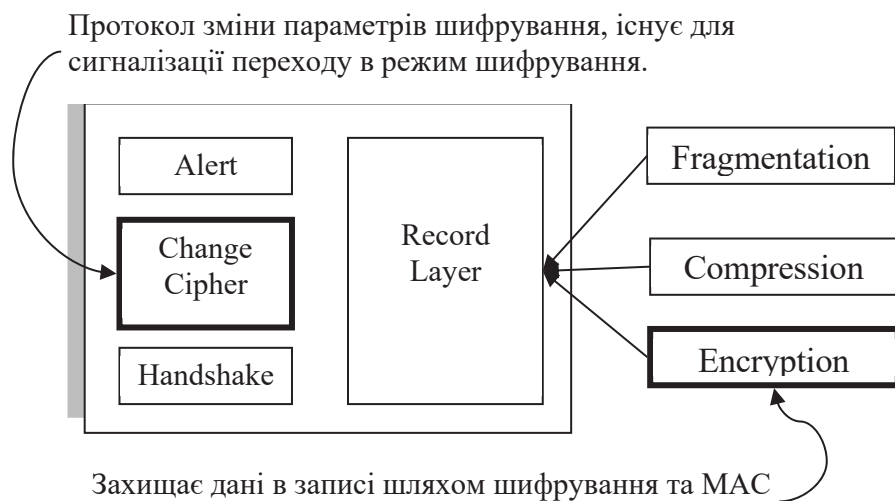


Рис. 13.35. Структура протоколу SSL

Протокол працює на двох рівнях. На першому Handshake Protocol Layer, який включає стек протоколів: протокол підтвердження підключення (Handshake Protocol), протокол зміни параметрів шифру (Change Cipher Spec Protocol), попереджувальний протокол (Alert protocol) забезпечується автентифікація та шифрування. На другому рівні використовується протокол запису [2, 48].



TLS Handshake Protocol

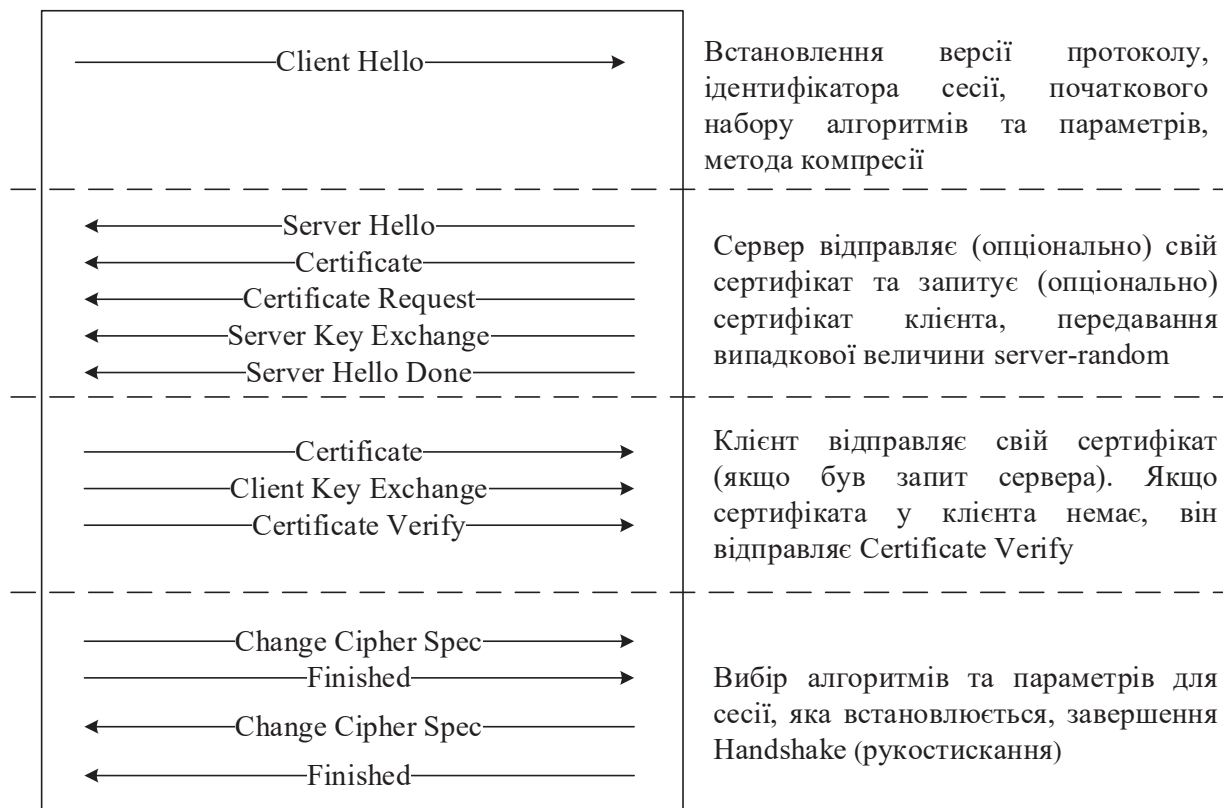


Рис. 13.37. Структурна схема роботи протоколу TLS

Проведений аналіз криптоалгоритмів, які використовуються в протоколі SSL/TLS показав, що криптоаналіз алгоритмів обмежується тільки потужністю системи, яка використовуваної для зламу, а при стрімкому розвитку комп'ютерних систем це лише питання часу. Найчастіше, клієнт має обмеження за потужністю системи, але не зловмисник [50].

13.4.3. Система PGP

Для забезпечення конфіденційності і сервісу автентифікації на прикладному рівні в комп'ютерних системах і мережах використовуються схеми PGP (Pretty Good Privacy) та S/MIME (Secure/Multipurpose Internet Mail Extension). Сервіс PGP, якщо не розглядати керування ключами, складається з п'яти функцій: автентифікація, конфіденційність, стиск, сумісність на рівні електронної пошти й сегментація (табл. 13.2).

Таблиця 13.2

Коротка характеристика функцій системи PGP

Функція	Алгоритми	Опис
Цифровий підпис	DSS/SHA або RSA/SHA	За допомогою SHA-1 створюється геш-код повідомлення. Отриманий у такий спосіб профіль повідомлення шифрується за допомогою DSS або RSA з використанням особистого ключа відправника й включається в повідомлення
Шифрування повідомлення	CAST або IDEA, або “потрійний” DES із трьома ключами й алгоритмом Діффі – Хеллмана або RSA	Повідомлення шифрується за допомогою CAST-128 або IDEA, або 3DES з одноразовим сеансовим ключем, який згенерований відправником. Сеансовий ключ шифрується за допомогою алгоритму Діффі – Хеллмана або RSA з використанням відкритого ключа одержувача й включається в повідомлення
Стиск	ZIP	Повідомлення можна стиснути для зберігання або передачі, використовуючи ZIP
Сумісність на рівні електронної пошти	Перетворення у формат radix-64	Щоб забезпечити прозорість для всіх додатків електронної пошти, шифроване повідомлення можна перетворити в рядок ASCII, використовуючи перетворення у формат radix-64
Сегментація	—	Щоб задовольнити обмеженням максимального розміру повідомлень, PGP виконує сегментацію й зворотне складання повідомлення

На рис. 13.38 показані основні схеми використання системи PGP.

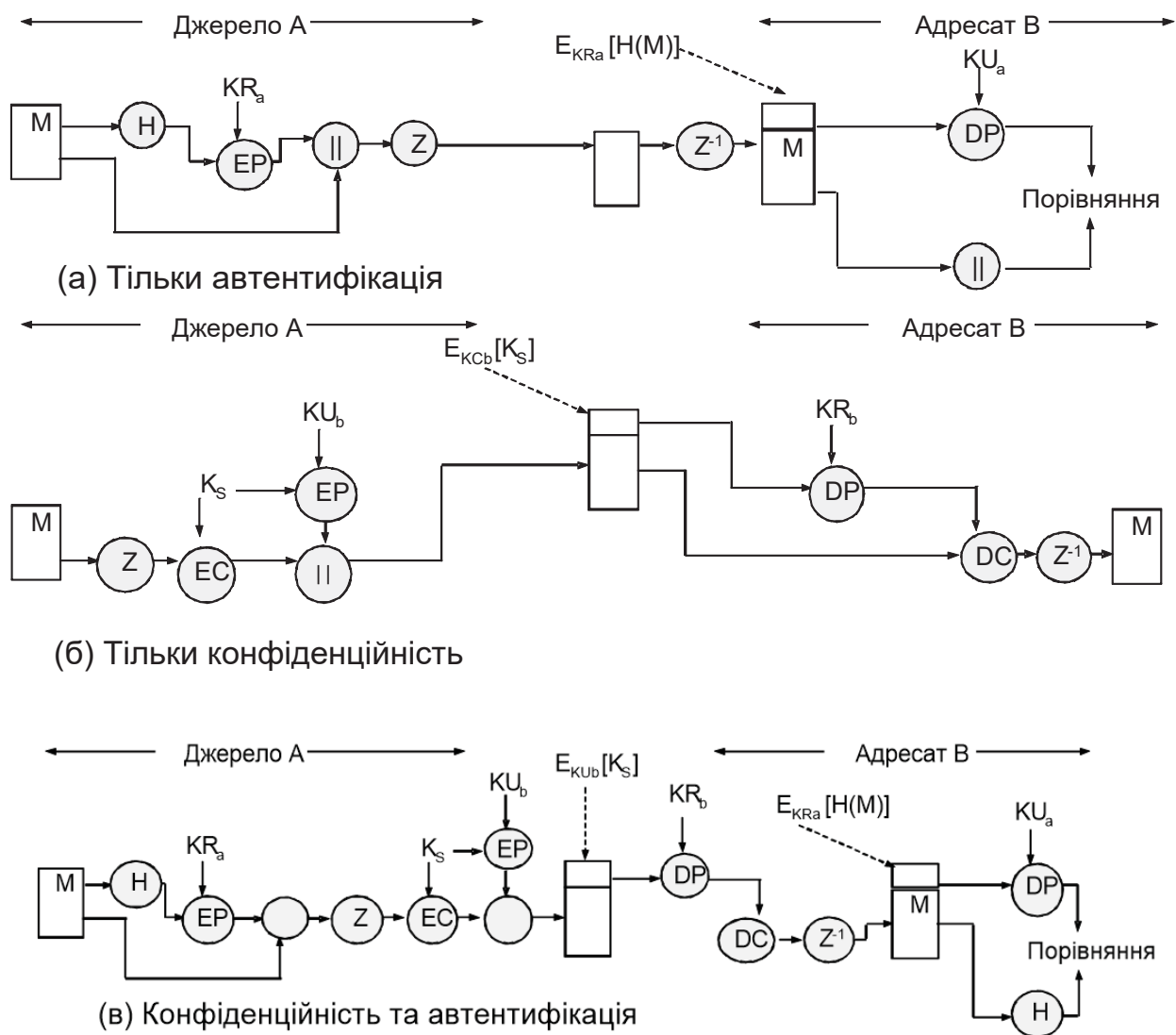


Рис. 13.38. Схеми використання системи PGP

Іншим основним сервісом, пропонованим PGP, є конфіденційність, забезпечувана шифруванням повідомлень, призначених для передачі або зберігання у вигляді файлів. В обох випадках можна використовувати традиційне шифрування за допомогою алгоритму CAST-128.

Альтернативою є застосування алгоритмів IDEA або 3DES. Може використовуватися й режим зворотного зв'язку шифрованих 64-бітових блоків (режим CFB).

Як завжди, необхідно вирішувати проблему розподілу ключів. У PGP кожний ключ схеми традиційного шифрування застосовується тільки один раз. Це значить, що для кожного повідомлення генерується новий ключ у вигляді випадкового 128-бітового числа. Таким чином, хоча в документації такий ключ називається сеансовим, насправді він є одноразовим. Через те що ключ задіється тільки один раз, такий сеансовий ключ приєднується до

повідомлення й передається разом з повідомленням. Щоб захистити ключ, він шифрується з використанням відкритого ключа одержувача.

Відправник генерує повідомлення й випадкове 128-бітове число, яке виступає в якості сеансового ключа тільки для цього повідомлення.

Повідомлення шифрується за допомогою алгоритму CAST-128 (або IDEA, або 3DES) і даного сеансового ключа.

Сеансовий ключ шифрується за допомогою алгоритму RSA і відкритого ключа одержувача й приєднується до початку повідомлення.

Одержувач використовує RSA з особистим ключем, щоб розшифрувати й тим самим відновити сеансовий ключ.

Сеансовий ключ застосовується для розшифрування повідомлення.

Щоб забезпечити альтернативу використанню RSA для шифрування ключа, в PGP пропонується параметр Diffie-Hellman (алгоритм Діффі – Гелмана). Алгоритм Діффі – Гелмана є алгоритмом обміну ключами. Насправді в PGP використовується варіант цього алгоритму з можливостями шифрування/розшифрування, відомий як алгоритм Ель Гамалія (Elgamal).

У зв'язку із цим можна зробити кілька зауважень. По-перше, щоб зменшити час шифрування, перевага віддається використанню комбінації традиційного шифрування й шифрування з відкритим ключем, а не простому використанню RSA або алгоритму Ель Гамалія, коли повідомлення шифрується безпосередньо: CAST-128 й інші алгоритми традиційної схеми шифрування значно швидші, ніж RSA або алгоритм Ель Гамалія. По-друге, використання алгоритмів схеми шифрування з відкритим ключем вирішує проблему розподілу сеансових ключів, тому що тільки для одержувача виявляється можливим відновити сеансовий ключ, приєднаний до повідомлення. У цій ситуації, скоріше, кожне повідомлення є незалежною одиночною подією зі своїм власним ключем. До того внаслідок самої природи електронної пошти, що є системою із проміжним зберіганням даних, використання процедури підтвердження зв'язку для того щоб переконатися в ідентичності сеансового ключа обох сторін, не є практично зручним розв'язком. Нарешті, використання одноразових ключів у традиційній схемі шифрування ще більш підсилює й без того досить надійний алгоритм традиційного шифрування. Тільки невеликий обсяг відкритого тексту шифрується з використанням одного ключа, і між ключами немає ніякого зв'язку. Таким чином, уся схема виявляється захищеною в тій мірі, у якій захищений алгоритм схеми шифрування з відкритим ключем. Тому PGP

пропонує користувачу вибір для довжини ключа від 768 до 3072 бітів (довжина ключа DSS для підписів обмежується завбільшки 1024 біти).

Як показано на рис. 13.38 (в), для одного повідомлення можна використовувати обидві служби. Спочатку для повідомлення у вигляді відкритого тексту генерується підпис, який додається в початок повідомлення. Потім відкритий текст повідомлення й підпис шифруються за допомогою алгоритму CAST-128 (або IDEA, або 3DES), а сеансовий ключ шифрується за допомогою RSA (або алгоритму Ель Гамала). Така схема переважніша зворотної, тобто схеми, коли спочатку шифрується повідомлення, а потім генерується підпис для шифрованого повідомлення. У загальному випадку виявляється більш зручним зберігати підпис із відкритим текстом повідомлення. До того ж з погляду можливостей тристоронньої верифікації, якщо спочатку генерується підпис, третій стороні не потрібно опікуватися про ключ традиційного шифрування, щоб перевірити підпис.

Отже, при використанні обох служб відправник спочатку підписує повідомлення за допомогою власного особистого ключа, потім шифрує повідомлення за допомогою сеансового ключа й, нарешті, шифрує сеансовий ключ за допомогою відкритого ключа одержувача.

За замовчуванням PGP стискає повідомлення після створення підпису, але перед шифруванням. Це має сенс із погляду зменшення обсягу даних як при передачі електронної пошти, так і при зберіганні у вигляді файлів. Дуже важливим виявляється вибір місця застосування алгоритму стиску, позначеного на рис. 13.38 як Z при стиску і як Z^{-1} при розпакуванні даних.

Підпис генерується до стиску за наступними ознаками:

1. Переважніше підписувати незжаті повідомлення, щоб у майбутньому мати можливість зберігати повідомлення в незжатому вигляді разом з підписом. Якщо підписати стислий документ, то для верифікації необхідно буде або зберігати стислу версію повідомлення, або стискати повідомлення щоразу, коли потрібна верифікація.

2. Навіть при наявності можливості динамічно повторно стискати повідомлення для верифікації. Такий підхід несе в собі додаткові труднощі через сам алгоритм стиску PGP: алгоритм не є детермінованим і різні реалізації алгоритму вибирають різні варіанти виконання для оптимізації співвідношення швидкості виконання й стиску, а в результаті виходять стислі файли різної форми. Такі різні алгоритми стиску є доступними через те, що будь-яка версія алгоритму може правильно відновити дані, отримані за допомогою будь-якої іншої версії. Застосування функції гешування й

створення підпису після стиску змусило б у всіх реалізаціях PGP застосовувати той самий алгоритм стиску.

Шифрування повідомлення застосовується після стиску для того, щоб підсилити криптографічний захист повідомлення. Через те що стисле повідомлення має меншу надмірність порівняно з оригінальним відкритим текстом, криптоаналіз виявляється більш важкою справою.

При використанні PGP шифрується, принаймні, частина переданого блоку. Якщо потрібний тільки цифровий підпис, то шифрується профіль повідомлення (з використанням особистого ключа відправника). Якщо має місце сервіс конфіденційності, шифрується (з використанням одноразового симетричного ключа) повідомлення плюс підпис (при наявності останньої). Таким чином, частина або весь вихідний блок повідомлення становить потік довільних 8-бітових байтів. Однак багато систем електронної пошти дозволяють використовувати тільки блоки, що складаються із символів тексту ASCII. Щоб задовольнити такому обмеженню, PGP забезпечує сервіс конвертування 8-бітового двійкового потоку в потік символів, що друкуються, ASCII.

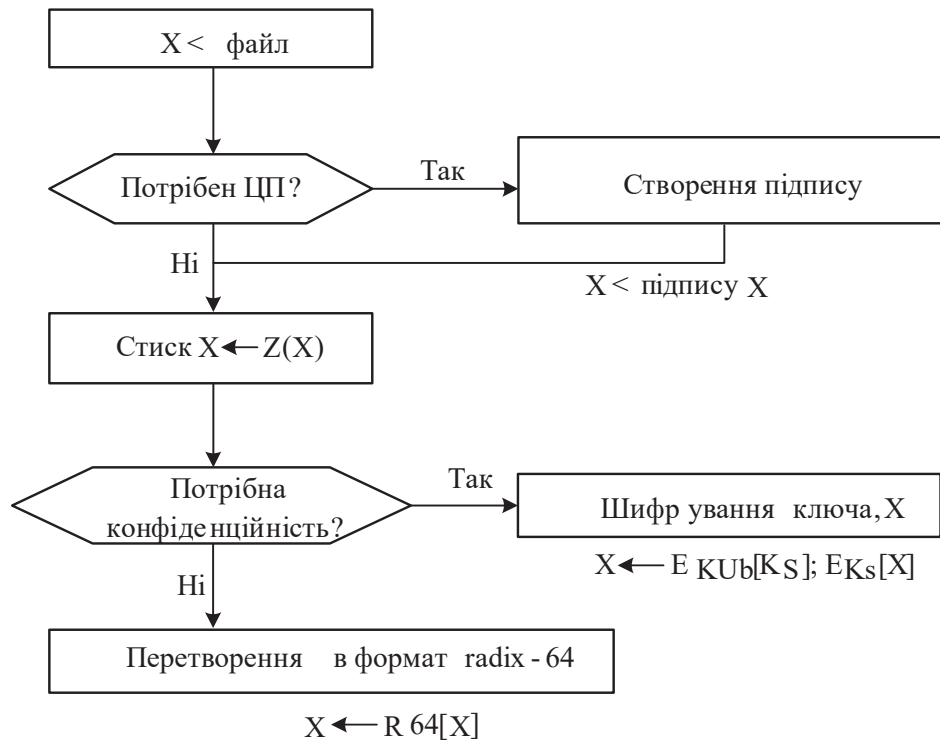
Для цього використовується схема конвертування radix-64. Кожна група із трьох байтів двійкових даних перетворюється в чотири символи ASCII, до яких приєднується контрольна сума (CRC), що дозволяє виявити помилки при передачі даних.

Конвертування у формат radix-64 збільшує довжину переданого повідомлення на 33 %. Сеансовий ключ і порція підпису повідомлення відносно компактні, а відкритий текст повідомлення стискається. Фактично стиск із надлишком компенсує розширення, яке одержане внаслідок перекладу у формат radix-64. Якщо ігнорувати відносно невеликий підпис і компоненти ключа, типовий повний вплив стиску та розширення для файлу довжини X повинен приблизно дорівнювати $1,33 \times 0,5 \times X = 0,665 \times X$. Таким чином, має місце загальний стиск, зразковий на одну третину.

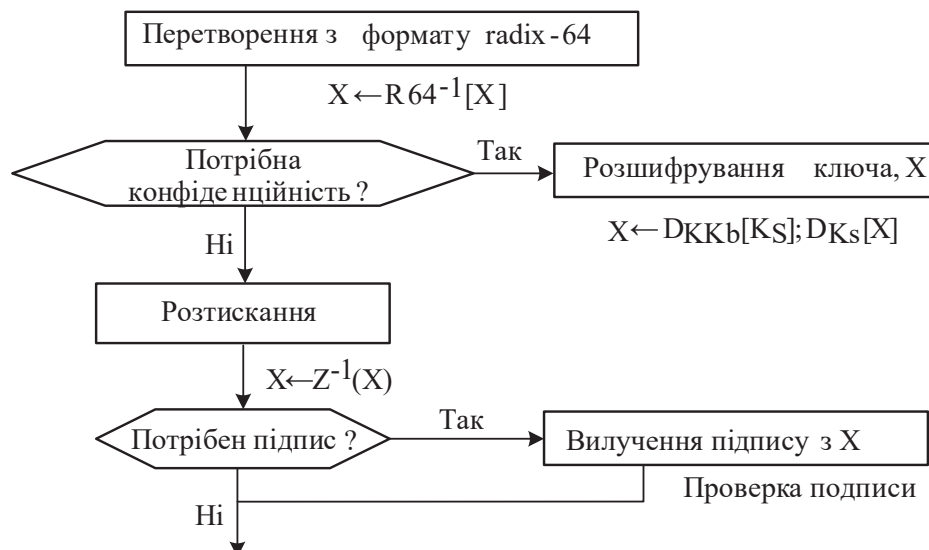
Аспектом, що заслуговує згадування алгоритму radix-64 є те, що він сліпо конвертує вхідний потік у формат radix-64, незважаючи на вміст, навіть якщо введення виявляється текстом ASCII. Таким чином, якщо повідомлення підписане, але не шифрується і конвертування застосовується до всього блоку, то вихідний потік даних буде незрозумілий випадковому спостерігачу, що вже забезпечує певний рівень конфіденційності. PGP можна конфігурувати так, щоб конвертування у формат radix-64 виконувалося тільки для порції підпису відкритого повідомлення. Це дає одержувачу

можливість прочитати повідомлення без використання PGP. Але PGP доведеться використовувати, якщо необхідно перевірити підпис.

На рис. 13.39 показаний зв'язок між чотирма описаними вище службами. При передачі, якщо це потрібно, підпис генерується за допомогою геш-коду відкритого тексту. Потім відкритий текст і підпис, якщо останній є, стискаються.



(а) Загальна схема відправлення (на стороні А)



(б) Загальна схема отримання (на стороні В)

Рис. 13.39. Відправлення й приймання повідомлень PGP

Далі, якщо потрібна конфіденційність, блок (стислий відкритий текст або стислі підпис і відкритий текст) шифрується й у початок додається шифрований відкритим ключем ключ шифрування традиційної схеми. Нарешті весь отриманий блок конвертується у формат radix-64.

На стороні одержувача вступний блок спочатку конвертується назад з формату radix-64 у двійковий. Потім, якщо повідомлення зашифроване, одержувач відновлює сеансовий ключ і дешифрує повідомлення.

Отриманий у результаті блок розтискається. Якщо повідомлення підписане, одержувач відновлює отриманий геш-код і порівнює його з геш-кодом, обчисленим ним самим.

Засоби електронної пошти часто обмежують максимально допустиму довжину повідомлення. Наприклад, багато засобів електронної пошти, доступні через Internet, допускають пересилання повідомлень довжиною не більше 50 000 байтів. Кожне довше повідомлення повинне бути розбите на сегменти меншої довжини, кожний з яких посилає окремо.

Щоб відповідати такому обмеженню, PGP автоматично розбиває занадто довгі повідомлення на сегменти, досить малі для того, щоб їх можна було переслати за допомогою електронної пошти.

Сегментація проводиться після виконання всіх інших операцій, включаючи перетворення у формат radix-64.

У результаті компонента ключі й підписи з'являються тільки один раз, на початку першого сегмента. На стороні одержувача система PGP повинна відкинути заголовок електронної пошти й знову зібрати весь оригінальний блок повідомлення перед виконанням кроків, показаних на рис. 13.39 (б).

Криптографічні ключі та зв'язування ключів

PGP використовує чотири типи ключів: одноразові сеансові ключі схеми традиційного шифрування, відкриті ключі, особисті ключі й паролльні ключі схеми традиційного шифрування, описані нижче. Відносно до цих ключів можна сформулювати наступні вимоги.

1. Наявність засобів генерування непередбачених сеансових ключів.
2. Бажано, щоб користувач міг мати декілька пар відкритих/особистих ключів. Однією із причин такої вимоги є те, що користувач може час від часу міняти пару ключів. У результаті всі повідомлення в шляху проходження виявляться створеними зі старим ключем. До того ж одержувачі будуть знати тільки старий відкритий ключ доти, доки ними не буде отримана нова версія ключа.

3. На додаток до необхідності час від часу міняти ключі. Користувач може мати декілька пар ключів одночасно, щоб взаємодіяти з різними групами одержувачів або просто для того щоб підсилити захист, обмежуючи обсяг матеріалу, шифрованого тим самим ключем. У результаті однозначної відповідності між користувачами і їх відкритими ключами немає.

Таким чином, виникає необхідність у засобах, що дозволяють ідентифікувати конкретні ключі.

Кожний об'єкт системи PGP повинен підтримувати файл власних пар відкритих/особистих ключів, а також відкритих ключів кореспондентів.

Розглянемо ці вимоги одна за одною.

Генерування сеансових ключів. Кожний сеансовий ключ зв'язується з одним повідомленням і використовується тільки для шифрування і розшифрування цього повідомлення.

Шифрування/розшифрування повідомлення виконується за допомогою алгоритму симетричної схеми шифрування. При цьому алгоритми CAST-128 і IDEA використовують 128-бітові ключі, а 3DES – 168-бітовий ключ. Припускаємо використання CAST-128.

Випадкові 128-бітові числа генеруються за допомогою самого алгоритму CAST-128. Введення для генератора випадкових чисел складається з 128-бітового ключа й двох 64-бітових блоків, які розглядаються як відкритий текст, що підлягає шифруванню. Використовуючи режим шифрованого зворотного зв'язку, шифрувальник CAST-128 породжує два 64-бітових блоки шифрованого тексту, які зв'язуються конкатенацією, у результаті чого формується 128-бітовий сеансовий ключ. Алгоритм, який при цьому використовується, заснований на алгоритмі, описаному в документі ANSI X12.17.

“Відкритий текст” для генератора випадкових чисел, сформований із двох 64-бітових блоків, вилучається з рандомізованого потоку 128-бітових чисел. Ці числа будуються на основі введення із клавіатури від користувача. Для створення рандомізованого потоку використовуються як час між натисканнями, так й інформація про фактично натиснуті клавіші. Таким чином, якщо користувач натискає випадкові клавіші у своєму звичайному темпі, буде породжений досить “випадковий” потік для введення. Це випадкове введення поєднується з попереднім сеансовим ключем, виданим алгоритмом CAST-128, щоб сформувати дані для введення генератора. У результаті через гарні властивості, що переміщують CAST-128,

породжується послідовність сеансових ключів, яка виявляється практично непередбаченою.

Ідентифікатори ключів. Шифроване повідомлення супроводжується використаним для шифрування сеансовим ключем у зашифрованому вигляді. Сеансовий ключ шифрується за допомогою відкритого ключа одержувача. Отже, тільки одержувач може розшифрувати сеансовий ключ і, таким чином, прочитати повідомлення. Якби кожний користувач використовував одну пару відкритого й особистого ключів, то відразу б знав, за допомогою якого із ключів можна дешифрувати сеансовий ключ – це єдиний особистий ключ одержувача. Однак ми висунули вимогу, щоб будь-який користувач міг мати будь-яку кількість пар відкритих/особистих ключів.

Як у цьому випадку одержувачеві довідатися, який з відкритих ключів використовувався для шифрування сеансового ключа? Найпростішим розв'язком є передача відкритого ключа разом з повідомленням. Одержувач міг би тоді впевнитися, що це дійсно один з відкритих ключів, і потім продовжити обробку повідомлення. Ця схема повинна працювати, але при цьому пересилається занадто багато зайвих даних. Відкритий ключ RSA може мати довжину в сотні десяткових розрядів. Іншим розв'язком є зв'язування з кожним відкритим ключем деякого ідентифікатора, унікального, принаймні, для одного користувача. Для цієї мети цілком підійде, наприклад, комбінація ідентифікатора користувача і ідентифікатора ключа. Тоді доведеться пересилати тільки значно коротший ідентифікатор ключа. Однак розв'язок породжує проблему керування і перевантаження: ідентифікатори ключів повинні приписуватись і зберігатись так, щоб як відправник, так і одержувач могли встановити відповідність між ідентифікаторами ключів і самими відкритими ключами. Це було б небажаним і обтяжним.

Розв'язком, прийнятим в PGP, є присвоєння кожному відкритому ключу такого ідентифікатора, який з дуже високою ймовірністю повинен виявитися унікальним для даного користувача. Ідентифікатор, що зв'язується з кожним відкритим ключем, розміщується в молодших 64 розрядах ключа. Це значить, що ідентифікатор відкритого ключа KU рівний ($KU \bmod 2^m$). Цієї довжини досить для того, щоб імовірність дублювання ідентифікаторів ключів виявилася дуже мала.

Ідентифікатор відкритого ключа відправника. Ідентифікує відкритий ключ, який повинен служити для розшифрування профілю повідомлення й,

отже, ідентифікує особистий ключ, що використовувався для шифрування профілю повідомлення.

Компонент повідомлення й необов'язковий компонент підпису можуть бути стиснуті за допомогою ZIP і можуть бути зашифровані з використанням сеансового ключа.

Компонент сеансового ключа включає сеансовий ключ і ідентифікатор відкритого ключа одержувача, який використовувався відправником для шифрування даного сеансового ключа.

Весь блок звичайно переводиться у форматі radix-64.

Ідентифікатори ключів PGP дуже важливі й включаються в будь-яке повідомлення PGP, що припускає, що ідентифікатор відкритого ключа KU рівний $KUA \bmod 2m$. Цієї довжини досить для того, щоб імовірність дублювання ідентифікаторів ключів виявилася дуже малою.

Ідентифікатор ключа потрібний і для цифрового підпису PGP. Через те що відправник може скористатися одним з декількох особистих ключів для шифрування профілю повідомлення, одержувач повинен знати, який відкритий ключ йому слід використовувати. Тому розділ цифрового підпису повідомлення включає 64-бітовий ідентифікатор відповідного відкритого ключа. При одержанні повідомлення одержувач перевіряє, що ідентифікатор відповідає відомому йому відкритому ключу відправника, а потім продовжує перевірку підпису. Тепер, визначивши поняття ідентифікатора ключа, можемо більш пильно розглянути формат переданого повідомлення, який показаний на рис. 13.40.

На рис. 13.40 подані такі позначення:

EKUB – шифрування з використанням особистого ключа для користувача В;

EKRA – шифрування з використанням відкритого ключа для користувача А;

EKS – шифрування з використанням сеансового ключа;

ZIP – функція стиску ZIP;

R64 – функція перетворення у формат radix-64.

Повідомлення складається із трьох компонентів: власне повідомлення, його підпису (необов'язково) і компонента сеансового ключа (необов'язково).

Компонент повідомлення включає фактичні дані, призначені для зберігання або передачі, а також ім'я файлу і мітку дати-часу, що вказує час створення повідомлення.



Рис. 13.40. Загальний формат повідомлення PGP (від А до В)

Компонент підпису включає наступні компоненти.

Мітка дати-часу. Час створення підпису.

Профіль повідомлення. 160-бітовий профіль повідомлення, створений за допомогою SHA-1 і шифрований з використанням особистого ключа підпису відправника. Профіль обчислюється для мітки дати-часу підпису, зв'язаного конкатенацією з порцією даних компонента повідомлення. Включення мітки дати-часу підпису в профіль забезпечує захист від атак відтворення повідомлення. Виключення імені файлу і мітки дати-часу компонента повідомлення гарантує, що відділений підпис буде в точності збігатися з підписом, що додається в префікс повідомлення. Відділені підписи обчислюються для файлу, у якому немає ніяких полів заголовка (хедера) повідомлень.

Ведучі два октети профілю повідомлення. Щоб забезпечити одержувачу можливість визначити, чи відповідний відкритий ключ використовувався для дешифрування профілю повідомлення з метою автентифікації, проводиться порівняння цих перших двох октетів відкритого тексту вихідного профілю з першими двома октетами дешифрованого профілю. Ці октети також служать 16-бітовою послідовністю, яка

використовується для перевірки повідомлення. Ідентифікатор відкритого ключа відправника. Ідентифікує відкритий ключ, який повинен служити для розшифрування профілю повідомлення й, отже, ідентифікує особистий ключ, що використовувався для шифрування профілю повідомлення.

Загальна структура зв'язування особистих ключів показана на рис. 13.41.

Мітка дати-часу	Ідентифікатор ключа*	Відкритий ключ	Шифрований особистий ключ	Ідентифікатор користувача*
• • •	• • •	• • •	• • •	• • •
Ti	$K_{ui} \bmod 2^{64}$	K_{ui}	$EN(P_i)[K_{ri}]$	Користувачі
• • •	• • •	• • •	• • •	• • •

Кільце відкритих ключів

Мітка дати-часу	Ідентифікатор ключа*	Відкритий ключ	Довіра власнику
• • •	• • •	• • •	• • •
Ti	$K_{ui} \bmod 2^{64}$	K_{ui}	trust_flagi
• • •	• • •	• • •	• • •

Ідентифікатор користувача*	Законність ключа	Підписи (підписи)	Довіра підпису (підписам)
• • •	• • •	• • •	• • •
Користувачі	trust_flagi		
• • •	• • •	• • •	• • •

(* – поле, використовуване для індексації таблиці)

Рис. 13.41. Загальна структура таблиці зв'язувань ключів

Ідентифікатор користувача. Звичайно тут розміщується адреса електронної пошти користувача (наприклад, `stallings@acm.org`). Однак користувач може вказати для кожної пари ключів різні імена (наприклад, Stallings, Wstallings, Williamstallings і т. п.) або використовувати один ідентифікатор користувача кілька разів.

Зв'язування особистих ключів може бути індексоване або за полем Ідентифікатор користувача, або за полем Ідентифікатор ключа.

Хоча передбачається, що зв'язування особистих ключів повинне зберігатися тільки на машині користувача, який створив й володіє відповідними парами ключів і що вона повинна бути доступна тільки цьому користувачу, має сенс зробити значення особистих ключів захищеними настільки, наскільки це можливо. Відповідно, сам особистий ключ у відкритому вигляді у зв'язуванні ключів не зберігається, а шифрується за допомогою CAST-128 (або IDEA, або 3DES). При цьому використовується наступна процедура.

Користувач вибирає фразу-пароль, яка використовується для шифрування особистих ключів.

Коли система за допомогою RSA генерує нову пару відкритого/особистого ключів, вона вимагає від користувача вказати таку фразу-пароль. З неї за допомогою SHA-1 генерується 160-бітовий геш-код, а потім пароль віддаляється.

Система шифрує особистий ключ за допомогою CAST-128, використовуючи 128 бітів геш-коду як ключа. Геш-код потім віддаляється, а шифрований особистий ключ зберігається у зв'язуванні особистих ключів. Згодом, коли користувач звертається до зв'язування особистих ключів, щоб витягти особистий ключ, йому доведеться знову вказати фразу-пароль. PGP витягне шифрований особистий ключ, обчислить геш-код пароля й дешифрує особистий ключ за допомогою CAST-128 з даним геш-кодом.

Це дуже компактна й ефективна схема. Як і в будь-якій заснованій на паролях системі, захищеність усієї системи залежить від захищеності пароля. Щоб не піддатися спокусі записати пароль, користувач повинен використовувати таку пароліну фразу, яку вгадати нелегко, а запам'ятати – просто.

На рис. 13.42 показана й загальна структура зв'язування відкритих ключів.

Ця структура даних дозволяє зберігати відкриті ключі інших користувачів, відомих даному. Проігноруємо деякі поля, зазначені в таблиці (див. рис. 13.41), і опишемо тільки частину з них.

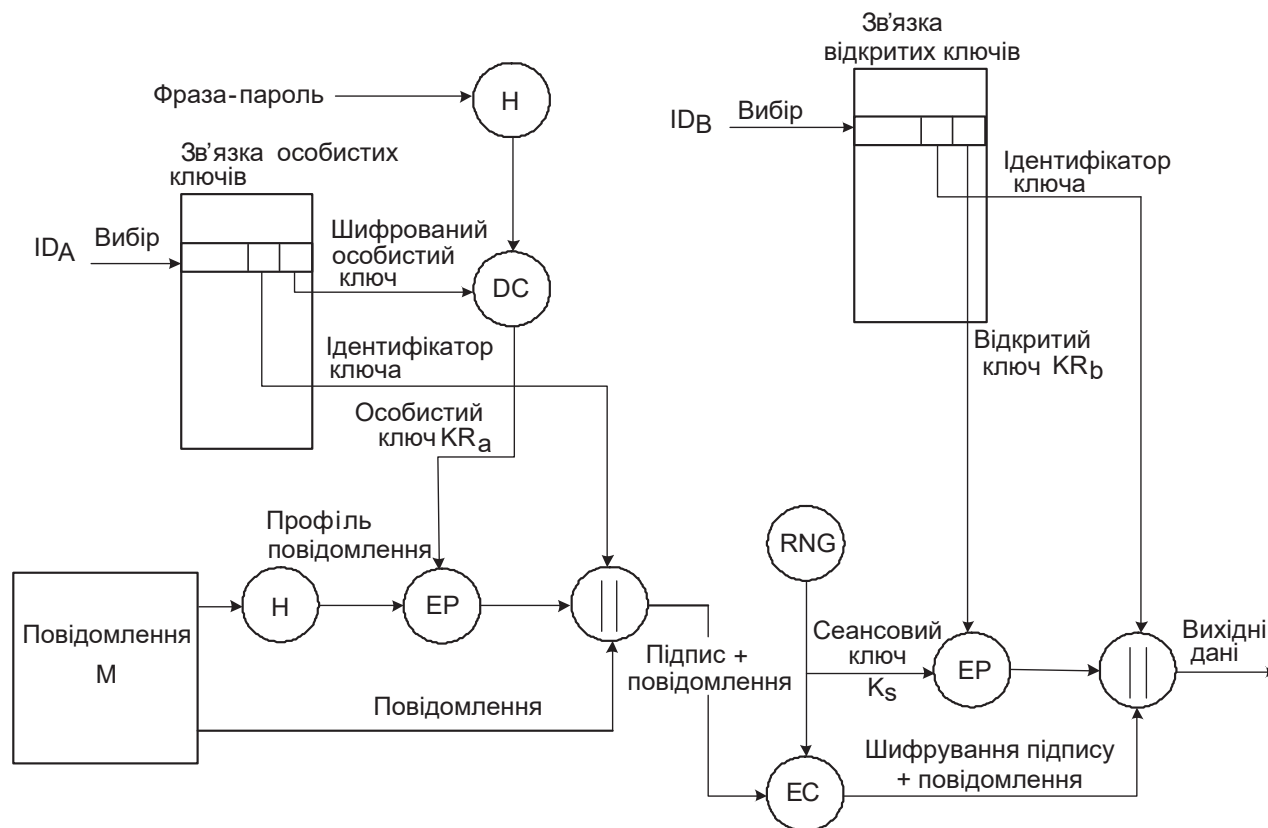


Рис. 13.42. Створення повідомлення PGP (від А до В, без стиску й перетворення у формат radix-64)

Мітка дати-часу. Дата й час створення даного запису.

Ідентифікатор ключа. Молодші 64 розряди відкритого ключа даного запису.

Відкритий ключ. Відкритий ключ даного запису.

Ідентифікатор користувача. Власник даного ключа. З одним відкритим ключем можна зв'язати кілька ідентифікаторів користувача.

Зв'язування відкритих ключів може бути індексоване або за полем Ідентифікатор користувача, або за полем Ідентифікатор ключа.

Для простоти в наступному прикладі проігноруємо стиск і перетворення у формат radix-64. Спочатку розглянемо передачу повідомлення (рис. 13.42), PGP виконує наступні кроки.

1. Створення підпису повідомлення.

PGP витягає особистий ключ відправника зі зв'язування особистих ключів, використовуючи введене значення `your_userid` у якості ключа

пошуку. Якщо відповідна команда не пропонує значення `your_userid`, вибирається перший особистий ключ у зв'язуванні.

PGP запитує в користувача фразу-пароль, щоб розшифрувати особистий ключ.

Створюється компонент підпису повідомлення.

2. Шифрування повідомлення.

PGP генерує сеансовий ключ і шифрує повідомлення.

PGP витягає відкритий ключ одержувача зі зв'язування відкритих ключів, використовуючи значення `her_userid` у якості ключа пошуку.

Створюється компонент сеансового ключа повідомлення.

Об'єкт, що ухвалює PGP, виконує наступні кроки (рис. 13.43).

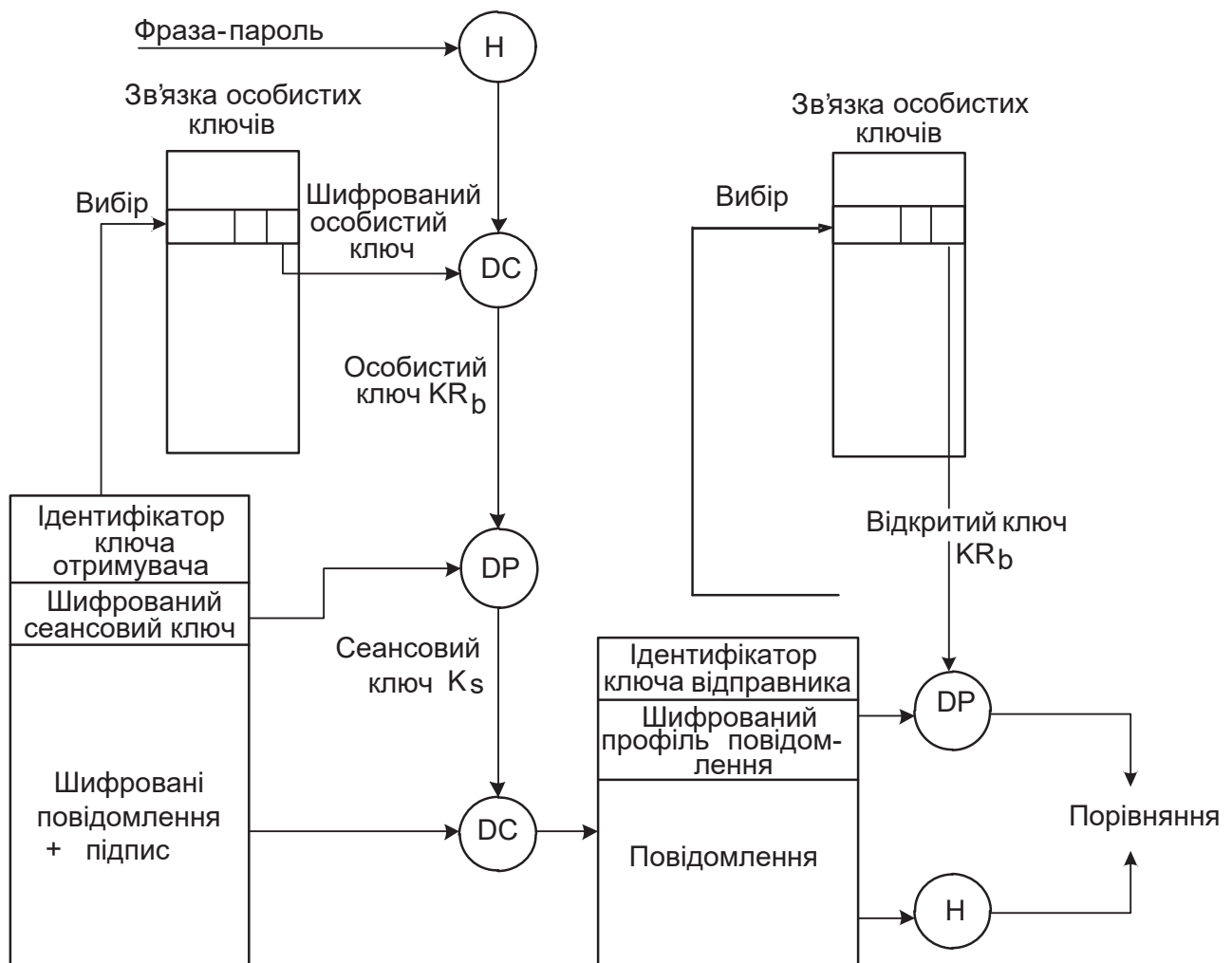


Рис. 13.43. Одержання повідомлення PGP (від А до В, без стиску й перетворення у формат radix-64)

3. Розшифрування повідомлення.

PGP витягає особистий ключ одержувача зі зв'язування особистих ключів, використовуючи в якості ключа пошуку значення поля Ідентифікатор ключа компонента сеансового ключа повідомлення.

PGP запитує в користувача фразу-пароль, щоб розшифрувати особистий ключ.

PGP відкриває сеансовий ключ і дешифрує повідомлення.

4. Автентифікація повідомлення.

PGP витягає відкритий ключ відправника зі зв'язування відкритих ключів, використовуючи в якості ключа пошуку значення поля Ідентифікатор ключа компоненти підпису повідомлення.

PGP відновлює отриманий профіль повідомлення.

PGP обчислює профіль повідомлення для прийнятого повідомлення й порівнює його із профілем, що прийшов разом з повідомленням, щоб переконатися в їх ідентичності.

Керування відкритими ключами. З наведеного вище опису PGP містить ясний і ефективний набір взаємозалежних функцій і форматів, що забезпечують надійну конфіденційність і засоби автентифікації. Для завершеності системи необхідно розв'язати ще одну проблему, а саме проблему керування відкритими ключами.

У документації PGP про важливість цієї проблеми говориться наступне.

Проблема захисту відкритих ключів від несанкціонованого втручання є окремою й найбільш складною практичною проблемою додатків, що використовують відкриті ключі. Це “ахілесова п'ята” криптографії з відкритим ключем, і значною мірою складність відповідного програмного забезпечення визначається складністю розв'язку саме цього завдання.

PGP пропонує структуру для розв'язку цієї проблеми й ряд опцій, які можуть при цьому використовуватися. Через те що система PGP призначена для використання в найрізноманітнішому середовищі, не встановлюється ніякої твердої схеми керування відкритими ключами, як, наприклад, це зроблено в системі S/MIME.

Суть проблеми полягає в наступному. Користувач А повинен побудувати зв'язування відкритих ключів, що містить відкриті ключі інших користувачів, щоб взаємодіяти з ними, використовуючи PGP. Припустимо, що зв'язування ключів сторони А включає відкритий ключ, приписаний стороні В, але насправді власником цього ключа є сторона С. Така ситуація,

зокрема, може мати місце, якщо учасник А взяв ключ із електронної дошки оголошень (BBS), яку учасник У використовував для того, щоб переслати відкритий ключ, але ключ був скомпрометований якимось С. У результаті виникла загроза за двома напрямками. По-перше, С може посилати повідомлення А, фальсифікуючи підпис В так, що А буде вважати повідомлення отриманим від В. По-друге, С може прочитати будь-яке шифроване повідомлення від А до В.

Для мінімізації ризику того, що зв'язування відкритих ключів користувача містить неправильні відкриті ключі, можна запропонувати кілька варіантів дій. Припустимо, що А потрібно одержати надійний відкритий ключ В. Декілька варіантів процедури, яку при цьому можна було б використовувати.

Одержання ключа від В особисто (фізично). Користувач У може зберегти свій відкритий ключ (Kub) на дискеті й вручити її користувачу А. Користувач А потім може завантажити такий ключ із дискети у свою систему. Це дійсно безпечний шлях, але він має свої очевидні обмеження.

Перевірка ключа по телефону. Якщо А може розпізнати В по телефону, то А може подзвонити В і попросити продиктувати ключ у форматі radix-64. Ще більш зручний варіант виглядає так: У може передати свій ключ користувачу А у вигляді електронного повідомлення. Користувач А може за допомогою RGP і з використанням SHA-1 згенерувати 160-бітовий профіль ключа й представити його в шістнадцятирічному форматі; такий профіль називається “відбитком” ключа. Після цього А може подзвонити В і попросити продиктувати рядок, відповідний до відбитка його ключа. Якщо два відбитки збігаються, ключ вважається перевіреним.

Одержання відкритого ключа У від надійного посередника D, який вселяє довіру обом сторонам. Для цього постачальник D створює підписаний сертифікат. Такий сертифікат повинен включати відкритий ключ В, час створення ключа й строк його дії. Сторона D генерує профіль SHA-1 цього сертифіката, шифрує його за допомогою свого особистого ключа й приєднує отриманий підпис до сертифіката. Через те що такий підпис створює тільки D, ніхто інший не зможе фальсифікувати відкритий ключ і заявити, що цей ключ був підписаний стороною D. Підписаний сертифікат може бути доставлений безпосередньо стороні А стороною В або D, або виставлений на електронній дошці оголошень.

Одержання відкритого ключа У від надійного вповноваженого вузла сертифікації. Сертифікат відкритого ключа створюється й підписується

вповноваженим вузлом. Користувач А може потім одержати доступ до такого вузла, вказавши своє ім'я користувача, і одержати підписаний сертифікат.

У цих випадках користувач А повинен уже мати екземпляр відкритого ключа постачальника сертифікатів і бути впевненим, що цей ключ надійний. В остаточному підсумку А повинен сам вирішити, наскільки надійною для нього є сторона, що виступає в ролі постачальника.

Хоча в системі PGP не висувається ніяких вимог відносно вибору вповноважених центрів сертифікації й ступенів довіри, PGP пропонує зручні засоби використання ступенів довіри, зв'язування ступенів довіри з відкритими ключами й інформацію про їх використання.

Базова схема має такий вигляд. Будь-який елемент у зв'язуванні відкритих ключів є сертифікатом відкритого ключа. З кожним таким елементом зв'язується поле відповідності ключа, яке задає ступінь довіри, з якого PGP буде вважати, що дійсним власником даного відкритого ключа є зазначений користувач: ніж вище ступінь довіри, тим сильніше прив'язка ідентифікатора користувача до даного ключа. Це поле обчислюється PGP. З кожним елементом зв'язується також якесь (можливо, нульове) число підписів для даного сертифіката, які були зібрані власником зв'язування ключів. У свою чергу, з кожним підписом зв'язується поле довіри підпису, що визначає ступінь, у якому PGP довіряє даному об'єкту підписувати сертифікати відкритих ключів. Значення поля відповідності ключа виводиться із сукупності значень полів довіри підпису для даного елемента зв'язування ключів. Нарешті, кожний елемент визначає відкритий ключ, що зв'язується з конкретним власником, а відповідне поле довіри власнику вказує ступінь довіри, з якого цей відкритий ключ може використовуватися для підпису інших сертифікатів відкритих ключів; цей ступінь довіри визначається й привласнюється користувачем. Значення полів довіри підпису можна розглядати як ґешовані копії значень полів довіри власнику інших елементів зв'язування ключів.

Три поля, що згадуються в попередньому абзаці, утримуються в структурі, яка називається байтом прапора довіри. Зміст цього прапора довіри для кожного з цих трьох полів показаний в табл. 13.3.

Допустимо, що ми маємо справу із зв'язуванням відкритих ключів користувача А. Операція визначення ступеня довіри може бути описана в такий спосіб.

Зміст байта прапора довіри

(а) Степінь довіри, приписуваний власнику відкритого ключа (розміщається після пакета інформації про ключ, визначається користувачем)	(б) Степінь довіри, приписуваний парі "відкритий ключ/ідентифіка-тор користувача" (розміщається після ідентифікатора користувача, обчислюється PGP)	(в) Степінь довіри, приписуваний підпису (розміщається після пакета підписів, кешована копія значення поля OWNERTRUST для даного постачальника підпису)
Поле OWNERTRUST - невизначена довіра; - невідомий користувач; - мінімальний рівень довіри для підпису; - середній рівень довіри для підпису; - максимальний рівень довіри для підпису; - даний ключ присутній у зв'язу-ванні секретних ключів (найвища довіра) Біт BUCKSTOP - встановлюється, якщо даний ключ присутній у зв'язуванні секретних ключів	Поле KEYLEGIT - невідома або невизначена відповідність; - ненадійна відповідність власнику ключа; - мінімально надійна відповідність власнику ключа; - повна відповідність власнику ключа Біт WARNONLY - встановлюється, якщо користувач бажає одержати тільки попередження, коли для шифрування використовується не повністю підтверджений ключ	Поле SIGTRUST - невизначена довіра; - невідомий користувач; - мінімальний рівень довіри для підпису; - середній рівень довіри для підпису; - максимальний рівень довіри для підпису; - даний ключ присутній у зв'язуванні секретних ключів (найвища довіра) Біт CONTIG - встановлюється, якщо підпис отримується по безперервному ланцюжку надійних сертифікатів до власника зв'язування ключів з найвищою довірою

1. Коли А додає новий відкритий ключ у зв'язування відкритих ключів, PGP повинна привласнити значення прапора довіри, пов'язаному із власником цього відкритого ключа. Якщо власником є А, і тому цей відкритий ключ повинен з'явитися також й у зв'язуванні особистих ключів, то полю довіри власника автоматично привласнюється значення найвищої довіри (ultimate trust). Інакше PGP запитує користувача А про те, який рівень довіри слід приписати власнику цього ключа, А повинен увести підходяще значення. Користувач може вказати, що цей власник невідомий, ненадійний, мінімально надійний або повністю надійний.

2. Коли додається новий відкритий ключ, до нього можна додати один або кілька підписів. Пізніше можна включити й інші підписи. Коли додається підпис, PGP виконує пошук у зв'язуванні відкритих ключів, щоб з'ясувати, чи значиться ім'я автора у цьому підписі серед відомих власників відкритих ключів. Якщо так, то значення поля OWNERTRUST цього власника привласнюється полю SIGTRUST даного підпису. А якщо ні, то відповідному ключу привласнюється значення невідомий користувач.

3. Значення поля відповідності ключа обчислюється на базі значень полів довіри підписів даного елемента зв'язування. Якщо принаймні один підпис має найвище (ultimate) значення у полі довіри підпису, то в поле відповідності ключа встановлюється значення повне (complete). Інакше PGP обчислює зважену суму значень полів довіри. Для підписів з максимальним рівнем довіри призначається вага $1/X$, а підписам із середнім рівнем довіри призначається вага $1/Y$, де X і Y є параметрами, що задаються користувачем. Якщо загальна сума ваг постачальників комбінацій “ключ/ідентифікатор користувача” досягає 1, то вважається, що відповідність надійна. Для поля відповідності ключа встановлюється значення повне (complete). Таким чином, за відсутності найвищої довіри для повної відповідності буде потрібно принаймні X підписів з максимальним рівнем довіри, або Y підписів із середнім рівнем довіри, або деяка їх комбінація, яка найбільше підходить.

Періодично PGP виконує перевірку зв'язування відкритих ключів, щоб підтримувати погодженість. По суті це спадний процес. Для кожного поля OWNERTRUST при такій перевірці PGP переглядає зв'язування, знаходить всі підписи, автором яких є даний власник, і обновляє значення полів SIGTRUST, щоб ці значення відповідали значенню поля OWNERTRUST. Увесь процес починається із ключів, для яких зазначена найвища довіра. Після цього значення всіх полів KEYLEGIT перераховуються на базі наявних підписів.

На рис. 13.44 показана зразкова схема зв'язування довіри підпису й відповідності ключа. Відображена структура зв'язування відкритих ключів. У цьому випадку користувач одержав кілька відкритих ключів, деякі безпосередньо від їх власників, а деякі – від третьої сторони, наприклад, із сервера ключів.

Вершина, позначена на рис. 13.44 “Ви”, представляє елемент зв'язування відкритих ключів, відповідний до даного користувача. Цей ключ, мабуть, відповідає власнику, тому значенням поля OWNERTRUST є найвища довіра.

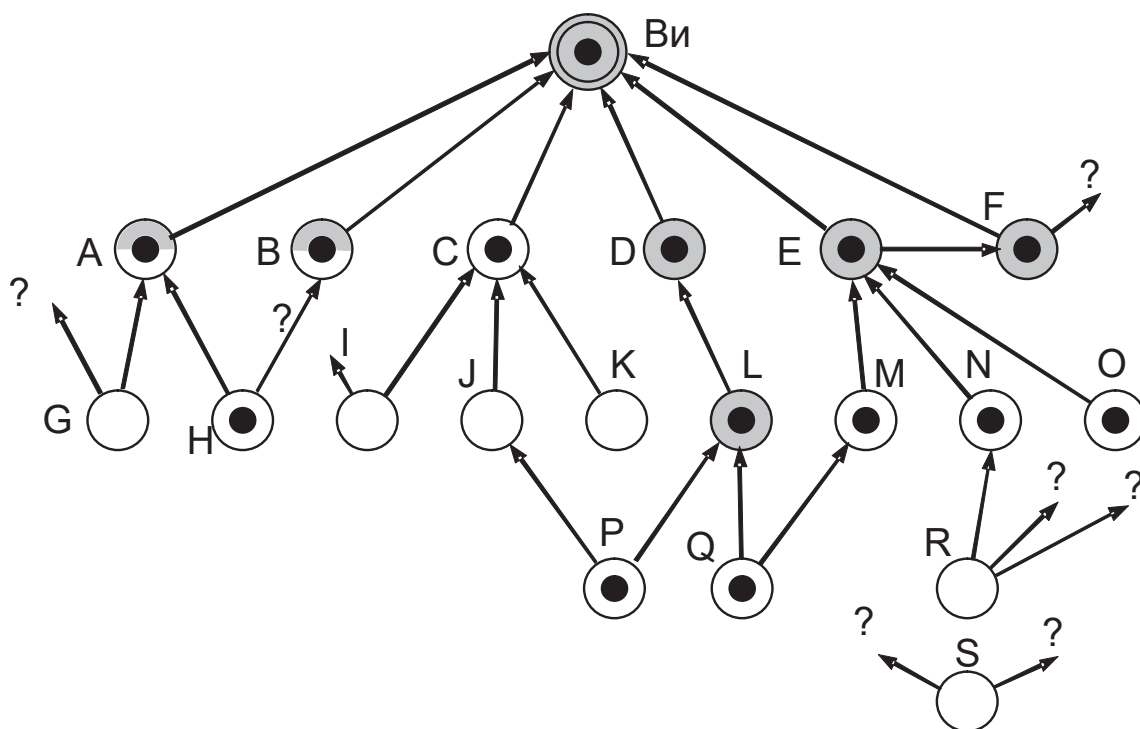


Рис. 13.44. Приклад моделі довіри PGP

- Умовні позначення:
- ? — невідомий власник;
 - $X \circ \rightarrow Y$ — X, підписаний Y;
 - — ви довіряєте власнику ключа;
 - ◐ — ви частково довіряєте власнику ключа;
 - ⊙ — ключ, що вважається вами правильним.

Для будь-якої іншої вершини поле OWNERTRUST у зв'язуванні ключів має значення невизначеної довіри, якщо тільки користувачем не задане деяке інше значення. У даному прикладі користувач указав, що він завжди довіряє підписувати інші ключі користувачам D, E, F і L.

Часткову довіру підписувати інші ключі одержали користувачі A і B.

Таким чином, зафарбування або його відсутність для вершин на рис. 13.44 указує рівень довіри, певної для цих користувачів. Деревоподібна структура говорить про те, якими користувачами були підписані відповідні ключі.

Якщо ключ був підписаний користувачем, чий ключ також присутній у даному зв'язуванні ключів, від підписаного ключа до ключа, що підписав

даний ключ користувачу, йде стрілка. Якщо ключ підписаний користувачем, ключа якого в даному зв'язуванні ключів немає, стрілка йде від підписаного ключа до знака питання, яка означає, що сторона, яка підписала ключ, даному користувачу невідома.

На рис. 13.44. проілюстровані наступні моменти.

Зверніть увагу на те, що всі ключі, власникам яких повністю або частково довіряє даний користувач, були підписані цим користувачем, за винятком вершини L. Такий підпис користувача не завжди необхідний, як у даному випадку, це має місце для вершини L, але на практиці більшість користувачів, швидше за все, підпишуть ключі більшості власників, яким вони довіряють. Тому, наприклад, навіть якщо ключ E вже був підписаний надійним постачальником F, користувач дозволів підписати ключ E особисто. Допустимо, що двох частково надійних підписів досить для того, щоб сертифікувати ключ. Отже, ключ користувача N розцінюється системою PGP як надійний (тобто відповідний до власника) через те, що він підписаний користувачами A і B, яким даний користувач частково довіряє. Ключ може бути визначений як надійний, якщо він підписаний однією цілком надійною або двома частково надійними сторонами, але може виявитися, що користувачу цього ключа не довіряють підписувати інші ключі. Наприклад, ключ N є надійним, оскільки він підписаний стороною E, якій даний користувач довіряє, але підписувати інші ключі стороні N не довіряє, оскільки даний користувач не привласнив N відповідне значення рівня довіри. Тому, хоча ключ R і підписаний стороною N, система PGP не вважає ключ R надійним. Така ситуація має зовсім певний зміст. Якщо ви прагнете послати секретне повідомлення деякому адресату, зовсім не обов'язково, щоб ви довіряли цьому адресату хоч якоюсь мірою. Необхідно, щоб ви були впевнені в тому, що маєте надійний відкритий ключ відповідного користувача.

На рис. 13.44 показаний також приклад окремої “вершини-сироти” S із двома невідомими підписами. Такий ключ міг бути отриманий із сервера ключів. PGP не може вважати цей ключ надійним тільки тому, що він прийшов з сервера, що має гарну репутацію.

Користувач повинен оголосити цей ключ надійним, підписавши його особисто або повідомивши PGP про те, що він готовий повністю довіряти одній зі сторін, що вже підписали даний ключ.

Таким чином, можна сказати наступне. Вище вже зазначалося, що з одним відкритим ключем у зв'язуванні відкритих ключів можна зв'язати

кілька ідентифікаторів користувачів. Це може мати місце, наприклад, у тому випадку, коли деяка сторона змінила своє ім'я або виступає за допомогою підписів під багатьма іменами, указуючи для себе, наприклад, різні адреси електронної пошти. Відкритий ключ має деяке число пов'язаних з ним ідентифікаторів користувачів з рядом підписів, асоційованих з кожним із цих ідентифікаторів. Прив'язка конкретного ідентифікатора користувача до ключа залежить від підписів, що зв'язуються із цим ідентифікатором користувача, тож степінь довіри даному ключу (для використання цього ключа з метою підписання інших ключів) виявляється функцією всіх відповідних підписів.

13.4.4. Система S/MIME

Система S/MIME забезпечує можливість пакування даних і цифровий підпис, сформований за допомогою шифрування профілю повідомлення, з використанням особистого ключа відправника.

У табл. 13.4 подані криптографічні алгоритми, які використовуються в системі S/MIME.

Система S/MIME є удосконаленням з погляду захисту стандарту формату MIME електронної пошти в мережі Інтернет, що базується на використанні технології RSA Data Security. Хоча PGP і S/MIME є стандартами IETF, існують підстави вважати, що S/MIME стане стандартом комерційного і промислового використання, тоді як PGP залишиться альтернативою для захисту особистої електронної пошти більшості індивідуальних користувачів.

З погляду загальних функціональних можливостей S/MIME і PGP дуже схожі. Обидві системи пропонують можливість підписувати та/або шифрувати повідомлення. S/MIME забезпечує можливість використання наступних функцій:

1. Упаковані дані. Складаються з шифрованого вмісту будь-якого типу і ключів шифрування вмісту для одного або більшого числа одержувачів.

2. Підписані дані. Цифровий підпис формується за допомогою обчислення профілю для вмісту повідомлення, яке вимагає підпису, і потім шифрується з використанням особистого ключа сторони, яка підписує цей вміст. Після цього вміст разом з підписом переводяться у формат base64. Повідомлення з підписаними даними може бути проглянуто тільки одержувачем, що має в своєму розпорядженні можливості S/MIME.

Криптографічні алгоритми в системі S/MIME

Функція	Вимоги
Створення профілю повідомлення, яке використовується при формуванні цифрового підпису	ОБОВ'ЯЗКОВА підтримка SHA-1 і MD-5. РЕКОМЕНДУЄТЬСЯ використання SHA-1
Шифрування профілю повідомлення для формування цифрового підпису	Для агентів відсилання й приймання ОБОВ'ЯЗКОВА підтримка DSS. Для агентів відсилання РЕКОМЕНДУЄТЬСЯ підтримка шифрування RSA. Для агентів приймання РЕКОМЕНДУЄТЬСЯ підтримка верифікації RSA з довжиною ключа від 512 до 1024 бітів
Шифрування сеансового ключа для передачі з повідомленням	Для агентів відсилання й приймання ОБОВ'ЯЗКОВА підтримка алгоритму Діффі – Гелмана. Для агентів відсилання РЕКОМЕНДУЄТЬСЯ підтримка шифрування RSA з довжиною ключа від 512 до 1024 бітів. Для агентів приймання РЕКОМЕНДУЄТЬСЯ підтримка дешифрування RSA
Шифрування повідомлення для передачі з використанням сеансового ключа	Для агентів відсилання РЕКОМЕНДУЄТЬСЯ підтримка шифрування triple DES і RC2/40. Для агентів приймання ОБОВ'ЯЗКОВА підтримка дешифрування triple DES і РЕКОМЕНДУЄТЬСЯ підтримка дешифрування RC2/40

3. Відкриті підписані дані. Як і у випадку підписаних даних, формується цифровий підпис вмісту. Проте в даному разі з використанням

base64 кодується тільки цифровий підпис. У результаті одержувачі без можливостей S/MIME зможуть проглянути вміст повідомлення, але не зможуть перевірити підпис.

4. Підписані й упаковані дані. Можливості підпису і упаковки можуть бути вкладені одна в іншу, так що шифровані дані можуть бути підписані, а підписані або відкриті підписані дані можуть бути зашифровані. S/MIME забезпечує перевірку достовірності даних, конфіденційність і цілісність повідомлень у форматі MIME. Робоча група Internet Engineering Task Force (IETF <<http://www.ietf.org>>) стандартизувала S/MIME 3.0 в документах Request for Comments (RFC) з номерами від 2632 до 2634. S/MIME – відмінний приклад гібридного рішення шифрування, в якому об'єднані достоїнства симетричного і асиметричного шифрів і функцій гешування. На рис. 13.45 показано етапи типового сценарію використання S/MIME.

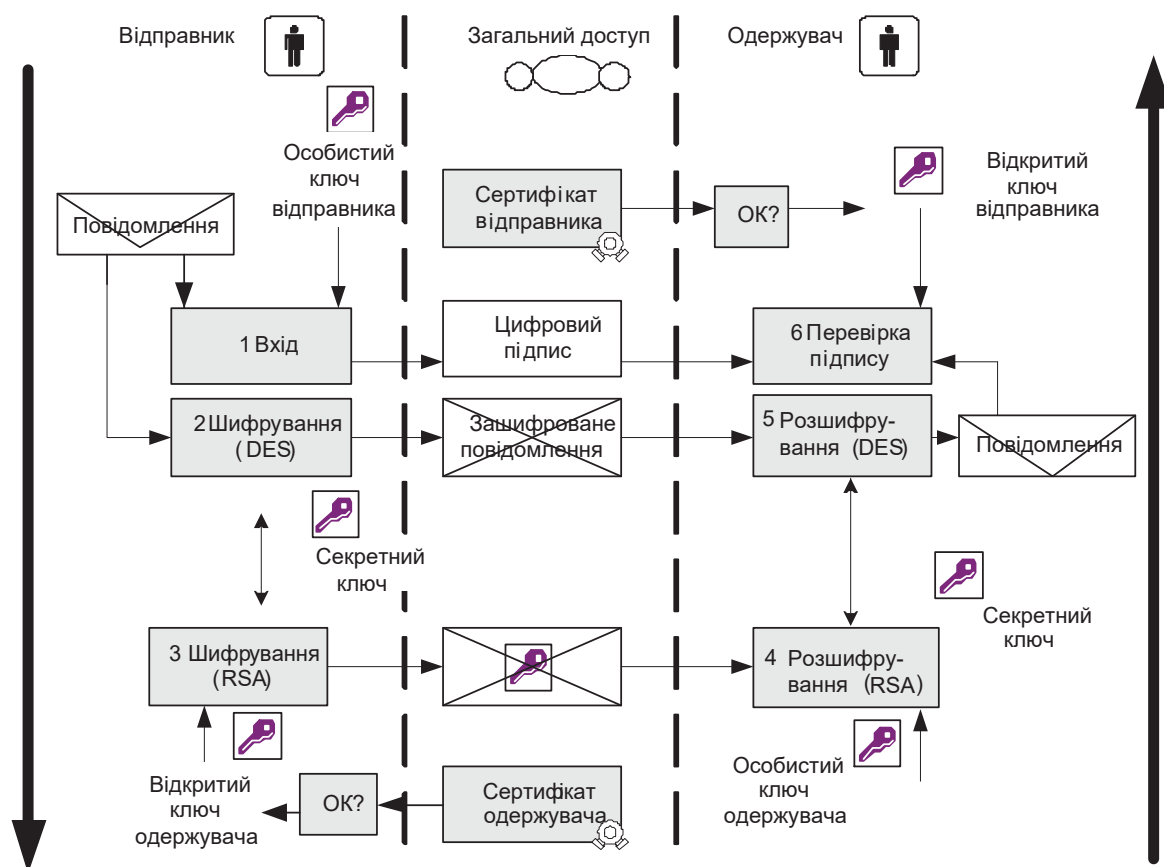


Рис. 13.45. Схема використання S/MIME для автентифікації забезпечення конфіденційності електронної пошти

Відправник хоче послати безпечне повідомлення (з гарантованою конфіденційністю, цілісністю, достовірністю даних) одержувачу.

Обмін S/MIME складається з наступних кроків:

Відправник створює цифрову сигнатуру для повідомлення з використанням свого приватного ключа.

Відправник використовує єдиний ключ симетричного шифрування для шифрування повідомлення.

Щоб сформувати безпечний канал, в якому буде захищена конфіденційність ключа шифрування при його передачі через загально-доступний канал зв'язку, відправник використовує відкритий ключ одержувача (з сертифікату одержувача), щоб зашифрувати ключ шифрування. Результат цього етапу – захищена скринька (lockbox), в якій міститься зашифрована копія ключа шифрування.

Одержувач використовує свій приватний ключ, щоб розшифрувати захищену скриньку. В процесі розшифрування формується єдиний ключ шифрування. Далі одержувач розшифровує повідомлення за допомогою єдиного ключа шифрування. Тепер він може прочитати повідомлення.

Одержувач використовує відкритий ключ відправника для перевірки достовірності і цілісності повідомлення та засвідчуючи цифрову сигнатуру, яка є в сертифікаті відправника. S/MIME забезпечує стійке крізне шифрування поштових повідомлень. Це значить, що при використанні S/MIME повідомлення зашифровані не тільки на етапі пересилки, але і при зберіганні в локальній особистій теці Microsoft Outlook (.pst) і поштової скриньці Microsoft Exchange Server.

Контрольні запитання

1. Концепція архітектурних засобів безпеки ISO.
2. Послуги безпеки. Їх розподіл за моделлю ISO.
3. Керування безпекою.
4. Функціональні вимоги безпеки.
5. Критерії адекватності систем безпеки. Профіль захисту.
6. Автентифікація джерела даних та об'єкта комунікацій.
7. Конфіденційність з'єднання трафіку, віддаленого поля даних.
8. Цілісність з'єднання з відновленням.
9. Профіль безпеки.
10. Сутність інформації як матеріальної цінності.
11. Конфіденційна інформація.

12. Архітектура системи захисту інформації.
13. Політика безпеки інформаційної системи.
14. Критерії захищеності інформаційної системи.
15. Загрози та ризики безпеки інформації.
16. Види пасивних та активних атак.
17. Класифікація загроз.
18. Основні вимоги до комп'ютерних мереж і систем.
19. Життєвий цикл розробки систем безпеки.
20. Порядок розробки профілю захисту і забезпечення безпеки.
21. Модель порушника безпеки.
22. Модель активної атаки.
23. Модель пасивної атаки.
24. Розподіл ключів. Сценарії розподілу ключів. Управління ключами.

ВИКОРИСТАНА ЛІТЕРАТУРА

1. Захист інформації в автоматизованих системах управління [Текст]: навч. посібник/ Уклад. І.А. Пількевич, Н.М. Лобанчикова, К.В. Молодецька. – Житомир: Вид-во ЖДУ ім. І. Франка, 2015. – 226 с.
2. Євсєєв С.П, Остапов С.Е., Король О.Г. Кібербезпека: сучасні технології захисту. Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678
3. Р.В. Гришук, та Ю.Г. Даник. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю.Г. Данника. Житомир: ЖНАЕУ, 2016.
4. С. Іванченко, В.О. Хорошко, Ю.Е.Хохлачова, та Д.В. Чирков під заг. ред. проф. В.О. Хорошка, “Забезпечення інформаційної безпеки держави”, К: ПВП “Задруга”, 2013.
5. Комутатор EX2200. URL: <https://stacl-system.com.ua/kommutator-juniper-ex2200-24p-4g>.
6. Комутатор EX3400. URL: <https://stacl-system.com.ua/kommutator-juniper-ex3400-24p>.
7. Маршрутизатор J2330. URL: <https://stacl-system.com.ua/marshrutezator-juniper-f2320-jh>.
8. Мережі на основі намірів. URL: https://www.cisco.com/c/ru_ru/solutions/intent-based-networking.html.
9. Мережеві рішення CISCO. URL: <https://www.cisco-parts.ru/catalog-cisco/setevye-resheniya-cisco>.
10. Міжмережевий екран SRX1000. URL: <https://stacl-system.com.ua/mezhsetevoj-jekran-juniper-srx1400base-xge-dc>.
11. Основи мережевих технологій. URL: https://www.cisco.com/c/ru_ru/solutions/small-business/resource-center/networking/networking-basics.html.
12. Сервер DL20 Gen10. URL: https://elmir.ua/servers/server_hp_proliant_dl20_gen10_p06477b21.html?gclid=Cj0KCQiAtqLBRC0ARIsAF4K3WGMLNrGVCMPpjg0oUW_source=gmerchant&utm_term=server_hp_proliant_dl20_gen10_p06477-b21.
13. Система управління ключами IBM Security GKLM. URL: <https://www.ibm.com/ru-ru/products/ibm-security-key-lifecycle-manager/details>.
14. Система управління ключами Key Manager Plus. URL: <https://www.manageengine.com/ru/key-manager>.

15. Стійка для серверів. URL: https://e-server.com.ua/servernye-stojki?pa_vysota.u=24&gclid=Cj0KCQIAAtqL.BRC0ARIsAF4K3WEG6xTR7Z9gww2T8aoT6bKyBq_zo_lXum_-OpD0TgF76KFn9rhLTMaAnAGEALw_wcB.

16. ДСТУ 4145–2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. – К. : Держстандарт України, 2002. – 40 с.

17. Жуков А.Е. Криптоанализ по побочным каналам (Side Channel Attacks) [Электронный ресурс] / А.Е. Жуков // Материалы конференции РусКрипто – 2006. – Режим доступа : – <http://www.ruscrypto.ru/sources/publications>.

18. О.О. Кузнецов, С.П. Євсєєв, С.В. Кавун, та О.Г. Король Сигнали і коди. Алгебраїчні методи синтезу. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

19. Євсєєв С.П. Кібербезпека: сучасні технології захисту. / Євсєєв С.П., Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678. – Режим доступу: <http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnologii-zakhystu.pdf>

20. Bonaventure O. Computer Networking: Principles, Protocols and Practice. – Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. – 272 p.

21. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, F. Vercauteren. Handbook of elliptic and hyperelliptic curve cryptography// Kenneth H. Rosen Ed. 2006. 843 p.

22. Edited by Serhii Yevseiev, Volodymyr Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p. URL:https://www.researchgate.net/publication/352013398_Synergy_of_building_cybersecurity_systems_Monograph

23. Антоненко О.В. Криптографічні методи перетворення інформації. Навчальний посібник для студ. вищ. пед. навч. закладів напряму підготовки 6.010104 Професійна освіта (Комп'ютерні технології). – Бердянськ: БДПУ, 2015. — 180 с.

24. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. – Львів : Видавництво Львівської політехніки, 2019. – 580 с. – ISBN 978-966-941-339-0.

25. X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. URL: <https://www.itu.int/rec/T-REC-X.509/en>.

26. Ленков С. В. Методы и средства защиты информации / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко; под ред. В. А. Хорошко. – В 2-х т. – К. : Арий, 2008. – Т.2. Информационная безопасность. – 344 с.

27. CCNA Cybersecurity Operations [Электронный ресурс]. – Режим доступа: <https://www.netacad.com/ru/courses/cybersecurity/cyberops-associate>. – 148 с.

28. Amazon Web Services (AWS) [Электронный ресурс]. – Режим доступа: <https://www.checkpoint.com/solutions/amazon-aws-security/>

29. Microsoft Azure (Azure) [Электронный ресурс]. – Режим доступа: <https://www.checkpoint.com/solutions/microsoft-azure-security>

30. ISO/IEC 10116, Information technology – Security techniques – Modes of operation for an n-bit block cipher. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:10116:ed-4:v1:en..>

31. Computer Network Security [Электронный ресурс]. – Режим доступа: <https://www.javatpoint.com/computer-network-security>

32. Google Cloud Platform (GCP) [Электронный ресурс]. – Режим доступа: <https://www.checkpoint.com/solutions/google-cloud-platform-security/>

33. Security requirements for cryptographic modules // URL: <https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf>.

34. Internet Security [Электронный ресурс]. – Режим доступа: https://www.tutorialspoint.com/internet_security/index.htm

35. Guide to LTE Security // URL: csrc.nist.gov/publications/drafts/80187/sp800_187_draft.pdf.

36. The Cybersecurity Framework // URL: [http://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf](https://csrc.nist.gov/publications/drafts/nistir-8170/nistir8170-draft.pdf).

37. Потий А. В. Стандартизация и сертификация в сфере защиты информации. Стандарты механизмов безопасности : учебное пособие / А. В. Потий. – Харьков : ХНУРЕ, 2002. – 80 с.

38. Проект RC5. – Режим доступа: <http://www.distributed.net/>.

39. В. А. Петин, Arduino и Raspberry Pi в проектах Internet of Things, ISBN: 978-5-9775-3646-2, 2016, 320 с. Режим доступа: <http://iisi.msu.ru/UserFiles/File/publications/>

40. Samuel Greengard, The Internet of Things (MIT Press Essential Knowledge series), ASIN: B00VB7I9VS, 2015, 230 P.

41. Cuno Pfister, Getting Started with the Internet of Things: Connecting Sensors and Microcontrollers to the Cloud (Make: Projects) 1st Edition, ASIN: B00COVJUGI, 2011, 194 P.

42. Erik Brynjolfsson and Andrew McAfee, The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies 1st Edition, ASIN: B00D97HPQI, 2014, 320 P.

43. Стеклов В. К. Проектування телекомунікаційних мереж: Підруч. для студ. вищ. навч. закл. за напрямком “Телекомунікації” / В.К. Стеклов, Л.Н. Беркман / за ред. В.К. Стеклова. – К.: Техніка, 2002. – 792 с.

44. Стеклов В.К. Телекомунікаційні мережі: Підруч. для студ. вищ. навч. закл. за напрямком “Телекомунікації” / В. К. Стеклов, Л. Н. Беркман. – К.: Техніка, 2001. – 392 с.

45. Thomas M. Siebel, Digital Transformation: Survive and Thrive in an Era of Mass Extinction, ASIN: B07SPDT74L, 2019, 253P.

46. Ethem Alpaydin, Machine Learning: The New AI (MIT Press Essential Knowledge series), ASIN: B01M60Y1T7, 2016, 232P

47. Таненбаум Э. Компьютерные сети. №3. – СПб.: Питер, 2002. – 848 с.

48. Хорошко В. А. Методы и средства защиты информации/ В. А. Хорошко, А. А. Чекатков. – К. : Юниор, 2003 – 504 с.

49. ANSI X9.63–1999 Public Key Cryptography For The Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography. – 1999. – 207 p.

50. Brassard J. Modern Criptolog / J. Brassard. – Berlin : Springer-Verlag, 1988. – 107 p. (Русский перевод: Современная криптология / Ж. Брассар. – М. : Полимед, 1999. – 176 с.).

51. Дудатьєв А.В., Каплун В.А., Семеренко В.П. Захист програмного забезпечення. Частина 1. Навчальний посібник. – Вінниця: ВНТУ, 2005. – 140 с.

52. Каплун В.А. Захист програмного забезпечення. Частина 2 : навчальний посібник. / В.А. Каплун, О.В. Дмитришин, Ю.В. Баришев – Вінниця: ВНТУ, 2014.

53. ISO/IEC 15408-1:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model [Electronic resource]. – Access mode: http://www.iso.org/iso/catalogue_detail.htm?csnumber=27632.

54. ISO/IEC 15408-3:2022. Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance

components [Electronic resource]. – Access mode:
<https://www.iso.org/ru/standard/72906.html>.

55. ISO/IEC 7498-2:1989 – Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture [Electronic resource]. – Access mode:
http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256.

56. Kerckhoffs A. La cryptographie militaire / A. Kerckhoffs // Journal des sciences militaires. – vol. IX. – P. 5–38 (Jan. 1883); P. 161–191 (Feb. 1883).

57. Matthews R. The use of genetic algorithms in cryptanalysts / R. Matthews // Cryptologia. –1993. – № 17(2). – P. 187–201.

58. Oppliger R. Contemporary Cryptography / R. Oppliger. – Artech House Publishers, 2005. – 510 p.

59. Schneier B. Applied Cryptography Second Edition: protocols, algorithms and source code in C. John Wiley & Sons Inc., 1996. (Русский перевод: Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М. : (ТРИУМФ, 2002.).

60. Security Pitfalls in Cryptography / B. Schneier // Cryptography Consultant Counterpane Internet Security, Inc., 2001.

61. Use of a Genetic Algorithm in the Cryptanalysis of Simple Substitution Ciphers // R. Spillman, M. Janssen, B. Nelson, M. Kepner. Cryptologia. – 1993. – № 17(1). – P. 31–44.

62. N. Ferguson. A Cryptographic Evaluation of IPsec. / Ferguson N., Schneier B. – 2003.

ЗМІСТ

ВСТУП.....	3
РОЗДІЛ 1. БАЗОВІ ТЕХНОЛОГІЇ ЛОКАЛЬНИХ МЕРЕЖ	4
1.1. Історія розвитку комп'ютерних мереж.....	4
1.2. Стандартизація в комп'ютерних мережах	5
1.3. Основні організації, що займаються стандартизацією комп'ютерних мереж.....	8
1.4. Еталонна модель взаємодії відкритих систем.....	10
РОЗДІЛ 2. ТЕХНОЛОГІЇ ФІЗИЧНОГО РІВНЯ.....	19
2.1. Середовища передавання даних.....	20
2.1.1. Мідний кабель.....	22
2.1.2. Волоконно-оптичний кабель.....	30
2.1.3. Бездротове з'єднання.....	32
РОЗДІЛ 3. ТЕХНОЛОГІЇ КАНАЛЬНОГО РІВНЯ.....	36
3.1. Підрівні Канального рівня IEEE 802 LAN/MAN.....	37
3.2. Стандарти каналного рівня	39
3.3. Фізичні та логічні топології.....	39
3.3.1. Топології WAN.....	40
3.3.2. Топології LAN	41
3.3.3. Застарілі LAN топології.....	42
3.3.4. Напівдуплексний та повнодуплексний зв'язок.....	43
3.3.5. Методи контролю доступу	44
3.3.6. Кадр.....	45
3.3.7. Адреси Рівня 2	47
РОЗДІЛ 4. ОСНОВНІ СТАНДАРТИ КОМП'ЮТЕРНИХ МЕРЕЖ.....	51
4.1. Технологія Ethernet (802.3)	51
4.1.1. Метод доступу CSMA/CD	53
4.1.2. Формати кадрів технології Ethernet.....	56
4.1.3. Специфікації фізичного середовища Ethernet	57
4.2. Технологія Token Ring (802.5).....	70
4.2.1. Маркерний метод доступу до середовища	75
4.2.2. Формати кадрів технології Token Ring (802.1)	77
4.3. Мережа Arcnet.....	81
4.4. Технологія FDDI	84
4.4.1. Особливості метода доступу технології FDDI.....	87
4.4.2. Порівняння з технологіями Token Ring та Ethernet	90
4.5. Високошвидкісна технологія Gigabit Ethernet	93
4.6. Технологія Wi-Fi.....	99
4.6.1. Фізичний рівень протоколів IEEE 802.11	100
4.6.2. Канальний рівень протоколів IEEE802.11. Технологія колективного доступу в дротових мережах.....	102
РОЗДІЛ 5. ХАРАКТЕРИСТИКИ МЕРЕЖНОГО РІВНЯ	106
5.1. Характеристики IP-протоколу.....	107
5.2. Пакет IPv4.....	108

5.3. Пакет IPv6	109
5.4. Адресація IPv4.....	111
5.4.1. Мережева та вузлова частина.....	111
5.4.2. Адреса мережі, адреса вузла та широкомовна адреса	113
5.5. Одноадресна, широкомовна та групова розсилки IPv4	115
5.5.1. Одноадресна розсилка	115
5.5.2. Широкомовна розсилка	115
5.5.3. Групова розсилка.....	116
5.6. Типи адрес IPv4.....	117
5.6.1. Публічні та приватні адреси IPv4	117
5.6.2. IPv4-адреси спеціального призначення	119
5.7. Механізм перетворення мережевих адрес (NAT).....	122
5.7.1. Типи NAT	125
5.8. Адресація IPv6.....	127
5.8.1. Формати адрес IPv6.....	128
5.8.2. Типи адрес IPv6	130
РОЗДІЛ 6. ОГЛЯД ПРОТОКОЛІВ МАРШРУТИЗАЦІЇ	139
6.1. Загальні характеристики	139
6.2. Алгоритм дистанційно-векторних протоколів	140
6.3. Удосконалені алгоритми вектора відстані	141
6.4. Протоколи стану каналу.....	143
6.5. Протокол BGP	145
6.6. Вибір шляху маршрутизатором.....	149
6.7. Статична маршрутизація.....	153
6.8. Статичні маршрути IPv6	154
РОЗДІЛ 7. СТАНДАРТНІ СТЕКИ КОМУТАЦІЙНИХ ПРОТОКОЛІВ	156
7.1. Стек TCP/IP	157
7.1.1. Реалізація міжмережної взаємодії засобами TCP/IP	157
7.1.2. Типи адрес стеку TCP/IP	159
7.1.3. Протоколи обміну маршрутною інформацією стека TCP/IP.....	166
7.2. Стек IPX/SPX	177
7.2.1. Загальна характеристика протоколу IPX	177
7.2.2. Формат пакету IPX.....	179
7.2.3. Маршрутизація протоколу IPX.....	183
7.3. Стек NetBIOS/SMB	185
7.4. Протоколи архітектури Apple Talk	187
7.5. Мережна архітектура NetWare	188
7.6. Протоколи архітектури SNA (фірми IBM).....	190
7.7. Мережна архітектура DNA	191
7.8. Безпека даних в IP-мережах.....	193
РОЗДІЛ 8. СТЕК ПРОТОКОЛІВ TCP/IP	196
8.1. Базова модель TCP/IP	196
8.2. Протоколи прикладного рівня.....	198
8.2.1 DNS (Служба доменних імен).....	200

8.2.2	Протокол динамічного налаштування вузла DHCP	202
8.2.3	Протоколи HTTP та HTTPS	205
8.2.4	Протокол передавання файлів (FTP)	205
8.2.5.	Протоколи обробки електронної пошти SMTP, POP3, IMAP4 ...	206
8.2.6.	Telnet, SSH та SNMP	208
8.3.	Протоколи транспортного рівня.....	210
8.3.1	Протокол TCP	211
8.3.2.	Протокол користувацьких дейтаграм UDP	215
8.3.3	Порти транспортного рівня	217
8.4.	Протоколи міжмережевого рівня	222
8.4.1	Протокол IP	223
8.4.2	Протокол ICMP	223
8.5.	Рівень мережного доступу	225
8.5.1.	Протокол ARP	225
РОЗДІЛ 9. ГЛОБАЛЬНІ КОМП'ЮТЕРНІ МЕРЕЖІ		229
9.1.	Основні поняття і визначення. Загальна структура й функції глобальних мереж	229
9.2.	Глобальний зв'язок на основі виділених ліній	231
9.2.1	Цифрові виділені лінії.....	231
9.3.	Глобальні мережі з комутацією каналів	243
9.3.1.	Стек протоколів і структура мережі ISDN	247
9.4.	Комп'ютерні мережі з комутацією пакетів	255
9.4.1.	Стек протоколів і структура мережі X.25	255
9.4.2.	Стек протоколів і структура мережі Frame Relay	257
9.4.3.	Стек протоколів і структура мережі ATM.....	259
9.4.4.	Інтерфейси DTE-DCE	263
9.4.5.	Введення в операції MPLS	266
9.4.5.	IP-телефонія	278
9.4.6.	Протоколи H.323	279
РОЗДІЛ 10. БЕЗДРОТОВІ КОМП'ЮТЕРНІ МЕРЕЖІ		291
10.1.	Переваги бездротового зв'язку	291
10.2.	Класифікація бездротових мереж	292
10.3.	Бездротові персональні мережі (WPAN).....	293
10.3.1.	Технологія IrDA.....	293
10.3.2.	Технологія Bluetooth	294
10.3.3.	Технологія зв'язку UWB	295
10.3.4.	Технологія зв'язку NFC.....	296
10.4.	Бездротові локальні мережі (WLAN)	297
10.4.1.	Огляд стандартів Wi-Fi.....	297
10.4.2.	Методи побудови мереж WLAN.....	298
10.4.3.	Організація безпеки WLAN.....	300
10.5.	Бездротові міські мережі (WMAN).....	301
10.6.	Бездротові глобальні мережі (WWAN)	302
10.6.1.	Радіорелейний зв'язок.....	302

10.6.2. Супутникові технології.....	304
10.6.3. Технології передавання даних в стільникових мережах.....	305
10.7 Протоколи інтернету речей.....	306
РОЗДІЛ 11. ОГЛЯД КАТЕГОРІЙ АТАК НА КОМП'ЮТЕРНІ МЕРЕЖІ ..	309
11.1. Загальна характеристика та принципи організації системи безпеки	309
11.2. Атаки доступу	310
11.3. Атаки модифікації	311
11.4. Атаки на відмову в обслуговуванні	312
11.5. Захист мережі з використанням брандмауерів	314
РОЗДІЛ 12. МЕТОДИ ЗДІЙСНЕННЯ АТАК НА ІНФОРМАЦІЙНІ МЕРЕЖЕВІ СИСТЕМИ.....	318
12.1. DoS-атаки.....	318
12.2. Прослуховування комутованих мереж (сніфінг).....	320
12.3. Імітація IP-адреси (IP-спуфінг)	322
12.4. Ін'єкції.....	323
12.5. Соціальний інжиніринг	324
РОЗДІЛ 13. СТАНДАРТИ МЕТОДІВ І ЗАСОБІВ ЗАХИСТУ В КОМП'ЮТЕРНИХ МЕРЕЖАХ.....	326
13.1. Побудова моделей порушника й атак на комп'ютерні мережі та системи.....	326
13.1.1. Аналіз умов функціонування та сучасних загроз інформації в комп'ютерних мережах та системах	326
13.1.2. Побудова класифікацій криптографічних засобів	331
13.1.3. Побудова моделі порушника безпеки в КМіС	345
13.1.4. Побудова моделі реалізації загроз безпеки в КМіС	357
13.1.5. Побудова математичної моделі пасивних атак у КМіС	360
13.1.6. Побудова моделі активних атак у КМіС із блокуванням передачі інформації.....	360
13.1.7. Побудова моделі активних атак у КМіС із внесенням перешкод	362
13.1.8. Побудова моделі активних атак “маскарад” у КМіС	363
13.2. Життєвий цикл розробки систем безпеки	374
13.2.1. Розробка профілю захисту і проекту безпеки об'єкта оцінки ...	374
13.2.2. Порядок розробки профілю захисту і проекту забезпечення безпеки.....	376
13.2.3. Структура і зміст профілю захисту	381
13.2.4. Структура і зміст проекту з забезпечення безпеки.....	383
13.2.5. Аналіз сучасних послуг й механізмів захисту інформації та визначення основних напрямків захисту КМіС.....	385
13.3. Національні і міжнародні стандарти криптографічного захисту інформації в ІС	388
13.3.1. Рекомендації стандарту ISO 7498-2	388
13.3.2. Загальні механізми забезпечення безпеки	405

13.3.3. Взаємозв'язок послуг та механізмів безпеки і взаємозв'язок послуг і рівнів моделі ВВС.....	407
13.3.4. Управління безпекою.....	411
13.4. Основні принципи захисту інформації при підключенні до мережі Інтернет.....	412
13.4.1. Захист інформації за допомогою міжмережних екранів.....	423
13.4.2. Захист інформації на мережному рівні.....	426
13.4.3. Система PGP.....	433
13.4.4. Система S/MIME.....	456
ВИКОРИСТАНА ЛІТЕРАТУРА.....	461

*Євсеєв С.П., Дженюк Н.В., Толкачов М.Ю.,
Король О.Г., Воронай Н.І.*

КОМП'ЮТЕРНІ МЕРЕЖІ

Книга 1. Технології комп'ютерних мереж

НАВЧАЛЬНИЙ ПОСІБНИК

*Керівник видавничого проєкту С.В. Піча
Дизайн та верстка К.А. Рижова*

Підписано до друку 24.11.2023
Формат 60х84 1/16. Папір офсетний. Цифровий друк.
Ум. друк. арк. 29,4375. Тираж 100.
Зам. № 2023-36

Видавництво ПП “Новий Світ-2000”
e-mail: novsv2000@gmail.com

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців і розповсюджувачів видавничої продукції: серія ДК № 59 від 25.05.2000 р., видане Державним комітетом інформаційної політики, телебачення та радіомовлення України.

Видавець ФОП Піча С.В.
а/с 5026, м. Львів-53, 79053, Україна
e-mail: novsv2016@ukr.net
e-mail: novsv2016@ukr.net, <https://ns2000.com.ua/>
+38 068-978-94-42, +38 050-337-58-46

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції: серія ДК № 5069 від 22.03.2016 року, видане Державним комітетом інформаційної політики, телебачення та радіомовлення України.