МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
“ДНІПРОВСЬКА ПОЛІТЕХНІКА”

ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ
Кафедра інформаційних систем та технологій

Гаркуша І.М.

Конспект лекцій
з дисципліни
“Комп’ютерні мережі”
для студентів галузі знань 12 “Інформаційні технології”
спеціальності 126 “Інформаційні системи та технології”

Дніпро
НТУ “ДП”
2019

УДК 004.07
Г20

Гаркуша І.М. Конспект лекцій з дисципліни “Комп’ютерні мережі” для студентів галузі знань 12 “Інформаційні технології” спеціальності 126 “Інформаційні системи та технології”. – Д.: НТУ «ДП», 2019. – 75 с.

В конспекті лекцій з дисципліни “Комп’ютерні мережі” для студентів спеціальності 126 “Інформаційні системи та технології” розглянуті загальні питання організації та функціонування комп’ютерних мереж, а також певних протоколів найвідомішого стеку протоколів TCP/IP.

Подані відомості щодо правил використання адресації вузлів IP-мереж, особливостей локальних технологій, а також таких технологій, як NAT, проксі-сервери та брандмауери.

Погоджено рішенням науково-методичної комісії спеціальності 126 Інформаційні системи та технології (протокол № 8 від 24.09.2019).

ЗМІСТ

ВСТУП

Метою дисципліни “Комп’ютерні мережі” для студентів спеціальності 126 “Інформаційні системи та технології” є формування компетентностей щодо оволодіння теоретичними знаннями та практичними навичками з моделювання та використання сучасних комп’ютерних мереж, а також знань, щодо архітектури мереж та їх функціонування, використання сучасного обладнання для побудови та захисту.

При складанні лекцій були використані матеріали широкого кола різноманітних навчально-методичних посібників та розробок, а також перевірена довідникова інформація з мережі Internet.

Лекційний курс є базою для подальшого вивчання процесу налаштування та адміністрування комп’ютерних мереж, а також корисний при пізнання певних технологій DevOps-інженірінгу.

Основними дисциплінарними результатами навчання, після завершення лекційного курсу “Комп’ютерні мережі”, є:

– вміння дати класифікацію комп’ютерної мережі, дати опис архітектури;

– обґрунтовано обирати архітектури комп’ютерної мережі та її складових;

– розуміння різновидів адресації мережевих вузлів та їх призначення;

– аргументовано обирати програмні та технічні засоби для створення мережних рішень інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи та експлуатаційних умов;

– володіння знаннями щодо використання технічних засобів комп’ютерних мереж;

– володіння знаннями щодо призначення та використання певних протоколів ком’ютерних мереж.

Лекція 1. Еволюція обчислювальних систем та мереж. Основні поняття та визначення

Концепція обчислювальних мереж (ОМ) є логічним результатом еволюції комп'ютерної технології. Перші комп'ютери 50-х років (великі, громіздкі та дорогі) були призначені для дуже невеликої кількості обраних користувачів. Такі комп'ютери не буди призначені для інтерактивної роботи користувачів, а використовувалися в режимі пакетної обробки.

Системи пакетної обробки, як правило, будувалися на базі мейнфрейму (рис. 1.1) – потужного та надійного комп'ютера універсального призначення. Користувачі готували перфокарти, які містили дані та команди програм, й передавали їх в обчислювальний центр. Оператори вводили ці картки в комп'ютер, а роздруковані результати користувачі отримували зазвичай тільки на наступний день.

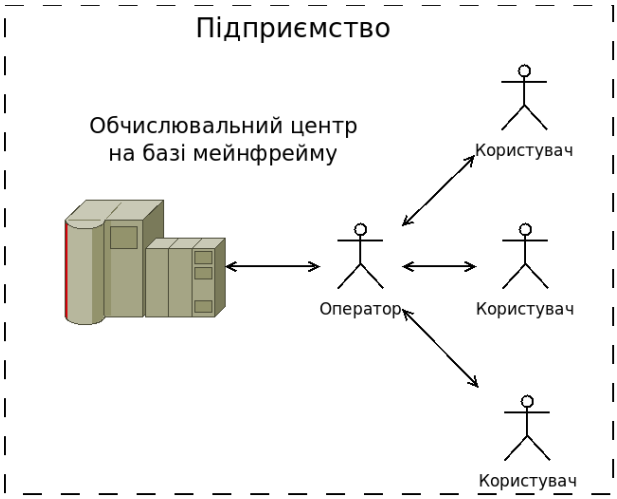

Рис. 1.1. Централізована система на базі мейнфрейму

В основі була ефективність роботи самого дорогого пристрою ЕОМ – процесору, в ущерб ефективності роботи спеціалістів, що його використовували.

По мірі здешевлення процесорів на початку 60-х років з'явилися нові способи організації обчислювального процесу, які дозволили враховувати інтереси користувачів. Почали розвиватися інтерактивні багатотермінальні системи розділення часу (рис. 1.2), прообрази обчислювальних мереж. В таких системах комп'ютер передавали у розпорядження відразу декільком користувачам. Кожний користувач отримував у своє розпорядження термінал, за допомогою якого він міг вести діалог з комп'ютером. Час реакції ОМ був достатньо малим для того, щоб користувачу була не сильно помітна паралельна робота з комп'ютером інших користувачів.

Такі багатотермінальні централізовані системи зовнішньо вже були дуже схожі на локальні ОМ (ЛОМ, ЛВС – рос.). Потреба підприємств у створенні ЛОМ на цей час ще не дозріла – в одній будівлі просто нічого було об'єднувати у мережу, оскільки через високу ціни на обчислювальну техніку, підприємства не могли себе дозволити розкіш купувати декілька комп'ютерів.

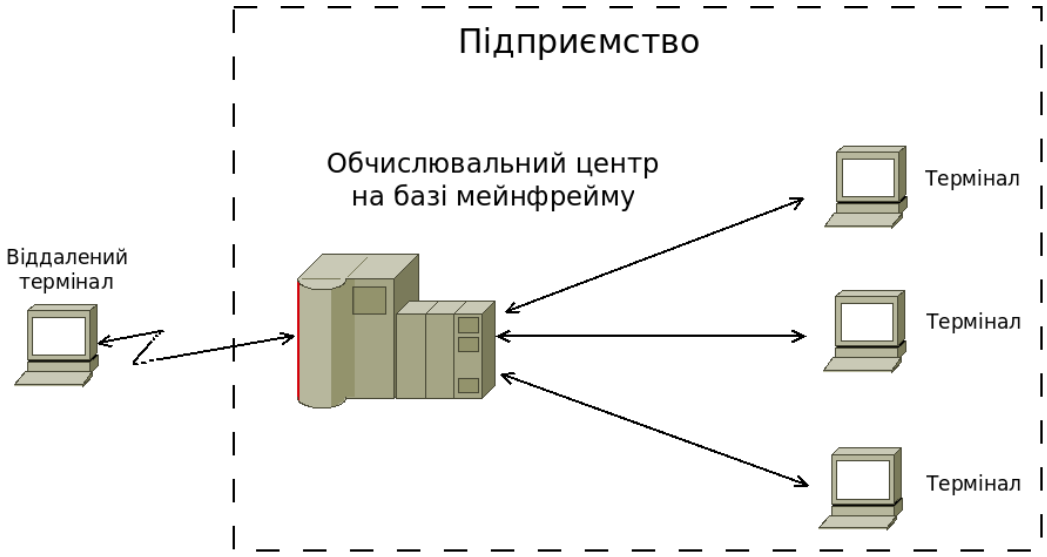

Рис. 1.2. Багатотермінальна система – прообраз обчислювальної мережі

В той період був справедливий так званий “закон Гроша”, який емпірично відображав рівень технології того часу. Згідно з цим законом працездатність комп'ютера була пропорційна квадрату його вартості. З цього виходило, що за одну й ту ж суму було вигідно купувати одну потужну машину, чим дві менш потужні – їх сумарна потужність була забагато нижча потужності дорогої машини.

Ти не менш, потреба у з'єднанні комп'ютерів, які знаходилися на великої відстані один від одного, до цього часу цілком назріла.

Почалося все з рішення більш простої задачі – доступу до комп'ютеру з терміналів, що були віддалені від нього на сотні та тисячі кілометрів. Термінали з'єднувалися з комп'ютерами через телефоні мережі за допомогою модемів. Потім з'явилися системи, в яких поряд з віддаленими з'єднаннями типу “термінал-комп'ютер” (Т-К) були реалізовані віддалені зв'язки типу “комп'ютер-комп'ютер”
(К-К). Комп'ютери отримали можливість обмінюватися даними в автоматичному режимі, що власно і є базовим механізмом любої ОМ.

З початку 70-х років розпочався технологічний прорив в області виробництва комп'ютерних компонентів – з'явилися великі інтегральні схеми (ВІС, БИС – рос.). Їх відносно невелика вартість та високі функціональні можливості привели до створення міні-комп'ютерів, які стали реальними конкурентами мейнфреймів. Закон “Гроша” перестав відповідати дійсності.

Навіть невеликі підрозділи підприємств отримали можливість придбати для себе комп'ютери.

Міні-комп'ютери виконували задачі управління технологічним обладнанням, складом та інші задачі рівня підрозділу підприємства. Таким чином, з'явилась концепція розподілу комп'ютерних ресурсів по всьому підприємству. Однак при цьому всі міні-комп'ютери однієї організації продовжували роботу автономно (рис. 1.3).

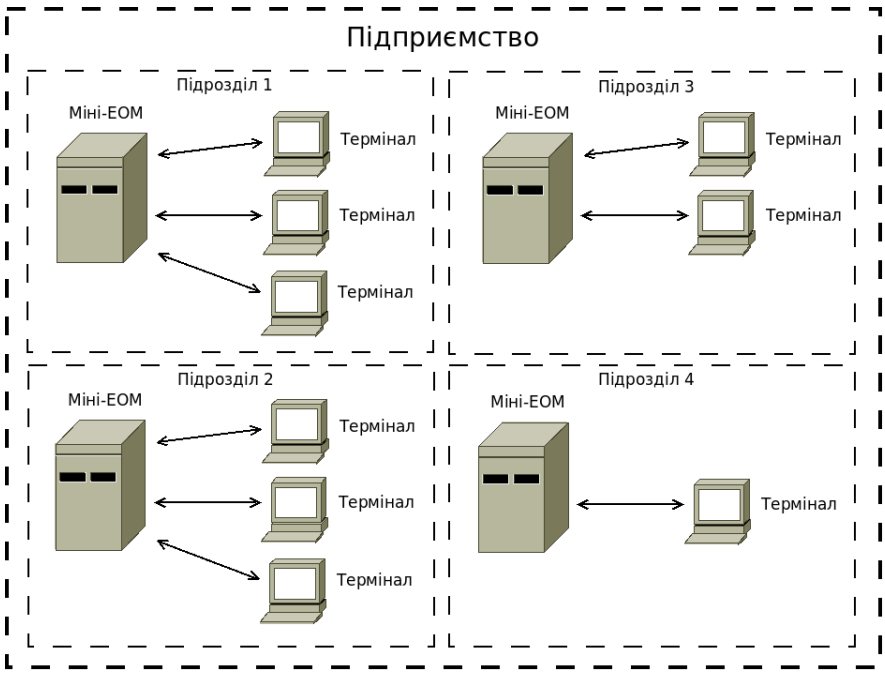

Рис. 1.3. Автономне використання декількох міні-комп'ютерів на одному підприємстві

Потреба в обміні даними між близько розташованими комп’ютерами призвела до з’єднання їх між собою та до розробки ПЗ, необхідного для їх взаємодії. Всі пристрої сполучення (рос. – сопряжения) на цьому етапі були різними.

В середині 80-х років положення справ в ЛОМ стало кардинально змінюватися. Затвердились стандартні технології об’єднання комп’ютерів в мережу – Ethernet, Arcnet, Token Ring. Міцним стимулом для їх розвитку стали персональні комп’ютери (ПК).

Сьогодні ОМ продовжують розвиватися досить швидко. Розрив між локальними та глобальними мережами постійно скорочується багато в чому за рахунок появи високошвидкісних територіальних каналів зв’язку, які не поступаються за якістю кабельним системам ЛОМ.

Комп’ютерна мережа (КМ) представляє собою систему розподіленої обробки інформації, яка складається як мінімум з двох комп’ютерів, які взаємодіють між собою за допомогою засобів зв’язку.

Комп’ютери, які входять у склад мережі, виконують достатньо широке коло функцій, основними з яких є наступні.

1. Організація доступу до мережі.
2. Управління передачею інформації.
3. Надання обчислювальних ресурсів та послуг абонентам мережі.

Засоби зв’язку націлені забезпечити надійну передачу інформації між комп’ютерами мережі. При розгляданні комп’ютерних мереж широко використовуються поняття клієнт та сервер.

На структурному рівні під сервером розуміється комп’ютер, який надає свої ресурси іншим комп’ютерам, що називаються клієнтами.

На програмному рівні під сервером та клієнтом розуміються процеси (програми), які виконують відповідно функції надання та використання мережевих ресурсів. Крім того, комп’ютери, за допомогою яких користувачі отримують доступ до ресурсів КМ, називають *робочими станціями* (РС).

Кожна КМ має певну архітектуру, яка, в свою чергу, визначається *топологією*, *протоколами*, *інтерфейсами*, *мережевими технічними та програмними засобами*. Кожна із складових архітектури КМ характеризує її окремі властивості і тільки їх сукупність характеризує всю мережу в цілому.

Топологія КМ відображає структуру зв’язків між її основними елементами. В силу ряду причин існує різниця між топологіями глобальних та локальних мереж.

Протоколи представляють собою правила взаємодії функціональних елементів мережі.

Інтерфейси – засоби сполучення функціональних елементів мережі. В якості функціональних елементів можуть виступати як окремі пристрої, так й програмні модулі. У відповідності з цим розрізняють апаратні та програмні інтерфейси.

Під *мережевими технічними засобами* розуміються пристрої, які забезпечують об’єднання комп’ютерів в єдину КМ. До цих пристроїв відносяться мережеві контролери, вузли комутації та інше обладнання.

Мережеві програмні засоби здійснюють управління роботою КМ та забезпечують відповідний інтерфейс з користувачами. До них відносяться мережеві ОС та допоміжні сервісні програми.

Основна мета мережі – забезпечити користувачам мережі потенційну можливість спільного користування ресурсами всіх комп’ютерів.

Перевагою ОМ є можливість розпаралелювання обчислень, за рахунок чого може бути досягнуто підвищення продуктивності та відмовостійкості системи. Використання ОМ дає підприємству наступні можливості.

1. Поділ дорогих ресурсів.
2. Удосконалення комунікацій.
3. Поліпшення доступу до інформації.
4. Швидке і якісне прийняття рішень.
5. Свобода в територіальному розміщенні комп'ютерів.

Класифікація КМ

Для класифікації КМ використовуються різні ознаки. Наприклад, найбільш відомими є:

– функціональне призначення комп'ютерів;

– територіальна ознака;

– масштаб виробничого підрозділу.

Відповідно до функціонального призначення комп'ютерів, мережі прийнято ділити на однорангові та мережі на основі серверів (серверні мережі).

В одноранговій мережі всі комп'ютери рівноправні, кожен з них може виступати в якості як клієнта, так і сервера. При цьому ресурси кожного комп'ютера умовно діляться на локальні та мережеві. Однорангова організація, як правило, використовується в невеликих мережах, що включають не більше 10 комп'ютерів.

У мережах на основі серверів виділяються окремі комп'ютери для серверів та клієнтів. Для кожного виду мережевих ресурсів може бути створений свій сервер, наприклад файловий сервер, сервер друку, сервер бази даних і т.п.

Найчастіше мережі ділять на типи за територіальною ознакою, тобто за величиною території, яку покриває мережа.

До *локальних мереж* – Local Area Network (LAN, ЛОМ, рос.: ЛВС) – відносять мережі комп'ютерів, зосереджені на невеликій території (зазвичай в радіусі не більше 1-2 км). Використовуються відносно дорогі високоякісні лінії зв'язку. Швидкості обміну можуть досягати 100 Мбіт/с. (1 Мбайт – 1024 Кбайт; 1 Мбіт – 10^6 біт). Реалізація в режимі on-line.

Глобальні мережі – Wide Area Network (WAN, ГОМ, рос.: ГВС) – об'єднують територіально розташовані комп'ютери, які можуть перебувати в різних містах та країнах. Для каналів зв'язку можуть використовуватися телефонні та телеграфні канали загального призначення, супутникові та оптоволоконні лінії зв'язку.

Міські, регіональні мережі (або мережі мегаполісів) – Metropolitan Area Network (MAN) – призначені для обслуговування території великого міста – мегаполісу. Вони займають проміжне положення між LAN та WAN і використовують цифрові магістральні лінії зв'язку, часто оптоволоконні. Вони застосовуються для зв'язку LAN в масштабах міста та їх з'єднання з WAN. Ці мережі можуть підтримувати такі послуги, як відеоконференції й інтегральну передачу голосу і тексту.

З кожним роком тенденція зближення LAN з WAN наростає.

За масштабом виробничого підрозділу виділяють наступні КМ.

Мережі відділів – це мережі, які використовуються порівняно невеликою групою співробітників, що працюють в одному відділі підприємства. Відділ

може налічувати до 100-150 співробітників. Головною метою мережі відділу є розділення локальних ресурсів, таких як програми, дані, лазерні принтери та модеми. Ці мережі зазвичай не розділяються на підмережі і створюються на якій-небудь одній мережевої технології.

Мережі кампусів – отримали свою назву від англійського слова campus – студентське містечко. Саме на території університетських містечок часто виникала необхідність об'єднання декількох дрібних мереж в одну велику. Зараз ця назва використовують для позначення мереж будь-яких підприємств та організацій. Однією з важливих служб, що надаються мережами кампусів, став доступ до корпоративних БД незалежно від того, на яких типах комп'ютерів вони розташовуються, а також використання загальних факс-серверів, високошвидкісних модемів та принтерів. Такі мережі розташовуються або в межах окремої будівлі або в межах однієї території, що покриває площу в кілька квадратних кілометрів. При цьому глобальні з'єднання в мережах кампусів не використовуються.

Корпоративні мережі (мережі масштабу підприємства) – об'єднують велику кількість комп'ютерів на всіх територіях окремого підприємства. Вони можуть бути складно пов'язані і покривати місто, регіон або навіть континент. Для таких мереж характерні:

– масштабованість – тисячі користувачів, сотні серверів, величезні обсяги збережених та переданих по лініях зв'язку даних, безліч різноманітних додатків;

– високий ступінь гетерогенності – типи комп'ютерів, комунікаційного обладнання, ОС та додатків різні;

– використання глобальних зв'язків – мережі філій з'єднуються за допомогою телекомунікаційних засобів, в тому числі телефонних каналів, радіоканалів, супутникового зв'язку.

Лекція 2. Топологія фізичних зв’язків

Під топологією КМ розуміється конфігурація графа, вершинам якого відповідають комп'ютери мережі (іноді й інше устаткування, наприклад концентратори), а ребрам – зв'язки між ними (рис. 2.1).

Конфігурація фізичних зв'язків визначається електричними з'єднаннями комп'ютерів між собою і може відрізнятися від конфігурації логічних зв'язків між вузлами мережі. Логічні зв'язки являють собою маршрути передачі даних між вузлами мережі й утворюються шляхом відповідної настройки комунікаційного обладнання.

Повнозв'язна топологія відповідає мережі, в якій кожен комп'ютер пов'язаний з усіма іншими.

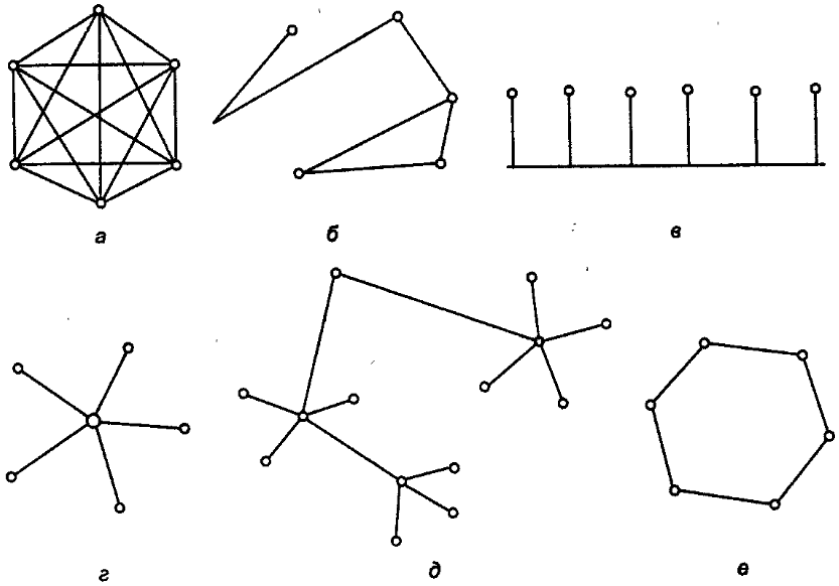

Рис. 2.1. Типові топології мереж: а) повнозв’язна топологія;
б) коміркова топологія (рос.: ячеистая), mesh-топологія;
в) загальна шина; г) топологія зірка;
д) ієрархічна зірка; е) кільцева топологія

Незважаючи на логічну простоту, цей варіант виявляється громіздким та неефективним, тому що кожен комп'ютер в мережі повинен мати велику кількість комунікаційних портів, достатню для зв'язку з кожним з інших комп'ютерів мережі. Для кожної пари комп'ютерів повинна бути виділена окрема лінія зв'язку.

Найчастіше цей вид топології використовується в багатомашинних комплексах або WAN при невеликій кількості комп'ютерів. Всі інші варіанти

засновані на неповнозв’язних топологіях, коли для обміну даними між двома комп'ютерами може знадобитися проміжна передача даних через інші вузли мережі.

Коміркова топологія (mesh) виходить з повнозв’язної видаленням деяких можливих зв'язків. У мережі з такою топологією безпосередньо зв'язуються тільки ті комп'ютери, між якими відбувається інтенсивний обмін даними, а для обміну даними між комп'ютерами, що не є з'єднаними прямими зв'язками, використовуються транзитні передачі через проміжні вузли. Коміркова топологія допускає з'єднання великої кількості комп'ютерів та характерна, як правило, для WAN.

Загальна шина (ЗШ) є поширеною топологією для LAN. Передана інформація може поширюватися в обидві сторони по шині. Застосування ЗШ знижує вартість проводки, уніфікує підключення різних модулів, забезпечує можливість майже миттєвого широкомовного звернення до всіх станцій мережі. Т.ч., основними перевагами такої схеми є дешевизна і простота розводки кабелю по приміщеннях. Недоліки – низька надійність, невисока продуктивність.

Топологія зірка. У цьому випадку кожен комп'ютер підключається окремим кабелем до загального пристрою, що зветься концентратором (HUB), який знаходиться в «центрі» мережі. У функції концентратора входить напрямок переданої комп'ютером інформації одному або всім іншим комп'ютерам мережі.

Головна перевага цієї топології перед ЗШ – істотно більша надійність. Крім того, концентратор може грати роль інтелектуального фільтра інформації, що надходить від вузлів в мережу та при необхідності може блокувати заборонені адміністратором передачі. До недоліків цієї топології відноситься більш висока вартість мережного устаткування через необхідність придбання концентратора. Крім того, можливості по нарощуванню кількості вузлів в мережі обмежується кількістю портів концентратора.

Іноді має сенс будувати мережу з використанням декількох концентраторів, ієрархічно з'єднаних між собою зв'язками типу зірка. На даний час ієрархічна зірка є найпоширенішим типом топології зв'язків як в LAN, так і в WAN.

У мережах з кільцевою топологією дані передаються по кільцю від одного комп'ютера до іншого, як правило, в одному напрямку. Якщо комп'ютер розпізнає дані як "свої", то він копіює їх собі у внутрішній буфер. У мережі з кільцевою топологією необхідно вживати спеціальні заходи, щоб в разі виходу з ладу або відключення будь-якої станції не перервався канал зв'язку між іншими станціями.

Кільце являє собою дуже зручну конфігурацію для організації зворотного зв'язку – дані, зробивши повний оборот, повертаються до вузла-джерела. Тому цей вузол може контролювати процес доставки даних адресату. Часто ця властивість кільця використовується для тестування зв'язності мережі та

пошуку вузла, що працює некоректно. Для цього в мережу посилаються спеціальні тестові повідомлення.

У той час як невеликі мережі, як правило, мають типову топологію – зірка, кільце або ЗШ, для великих мереж характерна наявність довільних зв'язків між комп'ютерами. У таких мережах можна виділити окремі, довільно зв'язкові фрагменти (підмережі), що мають типову топологію, тому їх називають мережами зі змішаною топологією.

Лекція 3. Методи доступу в локальних та глобальних мережах

Правило, за допомогою якого організовується доступ РС до передавального середовища (рос.: передающей среды), отримало назву *методу доступу*.

Залежно від методу доступу LAN діляться на дві групи. До першої групи належать мережі, в яких використовуються методи детермінованого доступу, до другої – методи випадкового доступу.

Метод *детермінованого доступу* (ДД) передбачає наявність певного алгоритму, на підставі якого РС надається доступ до передавального середовища. Алгоритм надання права передачі інформації може бути достатньо гнучким та враховувати пріоритети запитів на передачу і їх інтенсивність.

При використанні *методів випадкового доступу* кожна РС довільним чином, незалежно від інших систем, може звертатися до моноканалу. При цьому методі можливе одночасне звернення кількох РС до загального передавального середовища, тому даний метод доступу часто називають методом множинного доступу.

Методи доступу в мережах з шинної топологією

У мережах з шинної топологією використовуються обидва методи доступу. У разі одночасної передачі повідомлень декількома РС відбувається "зіткнення" повідомлень, що призводить до спотворення інформації. Тому в мережах з випадковим доступом кадр даних, щоб уникнути прийому помилкової інформації, доповнюється контрольною сумою. Приймаюча станція видає підтвердження тільки при прийомі кадрів з правильною контрольною сумою, інші кадри ігноруються. Це дозволяє передавальній станції контролювати передачу кадрів.

Удосконаленням цього методу з метою зниження конфліктів є попереднє прослуховування середовища передачі, та початок передачі тільки при наявності вільного каналу. Такий режим передачі отримав назву *множинного доступу з контролем несучої частоти* (МДКН або CSMA – Carrier Sense Multiply Access). Однак і в цьому випадку через кінцевий час поширення сигналів не можна повністю уникнути конфліктів.

З метою своєчасного виявлення конфліктів, РС, в процесі передачі інформації, постійно контролює передавальне середовище та при появі колізій (зіткнень) припиняє передачу. Через деякий проміжок часу після припинення передачі конфліктуючі РС здійснюють повторну спробу передачі інформації. Час затримки визначається за допомогою спеціальних алгоритмів, спрямованих на зниження ймовірності повторного конфлікту. Цей режим називається

МДКН/ВЗ (рос.: МДКН/ОС) або CSMA/CD (Carrier Sense Multiply Access/with collision detection), ВЗ – виявленням зіткнень (рос.: ОС – обнаружением столкновений).

Методи ДД можна розділити на методи поділу часу (МПЧ) та методи передачі повноважень (МПП).

Сутність МПЧ полягає в поділу часу роботи каналу зв'язку на окремі інтервали часу, кожен з яких, згідно з визначеним правилом, надається будь-якої РС. Більшість МПЧ передбачає наявність в мережі диспетчера, основною функцією якого є контроль та планування часу доступу. При цьому з'являється можливість враховувати пріоритети і необхідний час взаємодії РС.

У МПЧ розглядають методи синхронного (циклічного) поділу та методи асинхронного поділу часу. При використанні другого різновиду МПЧ підвищується ефективність використання моноканалу.

МПП (метод маркерного доступу) полягає в тому, що послідовно від однієї РС до наступної передається маркер (певна послідовність бітів). РС розміщують свої повідомлення за маркером і передають маркер з повідомленням до наступної РС і т.д. Приймає повідомлення тільки одержувач. Передача кадрів даних здійснюється в обох напрямках в моноканалі. У мережах з таким методом доступу доводиться постійно відстежувати втрату маркера або появу кількох маркерів.

Методи доступу в локальних кільцевих мережах

Основні методи – метод тактируємого доступу та метод маркерного доступу. Перший метод передбачає розбиття тимчасового циклу кільця, тобто часу поширення сигналу по кільцю, на безліч рівних інтервалів часу – тактів (сегментів), в кожен з яких поміщається по одному кадру даних. Таким чином одночасно можуть передаватися кілька кадрів. Кількість та довжина кадрів визначається з урахуванням основних характеристик мережі. РС може передавати інформацію в кільце тільки при проходженні через її блок доступу вільного кадру. Звільнення (обнулення) кадрів може здійснюватися як одержувачем, так і відправником інформації.

Кращим є метод маркерного доступу, основна відмінність якого від такого ж методу, але в мережах з шинної топологією, полягає в тому, що кадри маркера та даних передаються по фізичному кільцю в одному напрямку. Видалення прийнятих кадрів, як правило, здійснюється передавальної РС.

Передача інформації в глобальних мережах

Основою WAN є мережа передачі даних, що представляє собою сукупність каналів передачі даних та вузлів комутації. У зв'язку з цим однією з визначальних характеристик WAN є спосіб комутації даних.

Залежно від способу комутації розрізняють мережі з комутацією каналів, комутацією пакетів, комутацією повідомлень та інтегральні мережі передачі даних.

При *комутації каналів* інформація від відправника до одержувача передається тільки після відправки відправником відповідного повідомлення про бажання встановити зв'язок та відправці одержувачем відповідного повідомлення про готовність почати прийом інформації. При передачі самої інформації до каналу не можуть звертатися інші бажаючі. Канал залишається зайнятим на весь сеанс обміну інформацією. Після закінчення обміну інформацією відправник виробляє відповідне керуюче повідомлення про роз'єднання та закінчення сеансу обміну інформацією. Коефіцієнт використання каналу низький.

Мережі з комутацією каналів можна розділити на два класи – мережі з динамічною комутацією та мережі з постійною комутацією. В наведеному вище прикладі представлено динамічну комутацію (з ініціативи користувача). У другому випадку з'єднання встановлюється не користувачем, а персоналом, який обслуговує мережу. Режим постійної комутації в мережах з комутацією каналів часто називають сервісом виділених (dedicated) або орендованих (leased) каналів.

Передача інформації за допомогою так званої, *комутації пакетів* здійснюється без виконання фізичного з'єднання між пунктами відправлення та отримання інформації. Між ними встановлюється віртуальне (логічне) з'єднання, а фізичний канал встановлюється локально між суміжними вузлами комутації і тільки на час передачі даних. При цьому інформація може надаватися і передаватися у вигляді блоку даних фіксованої структури та довжини. Заголовок блоку даних містить адреси відправника та одержувача, а також іншу інформацію для управління та коректної передачі повідомлень між абонентами. Передача блоків даних між абонентами здійснюється з проміжним запам'ятовуванням їх у вузлах комутації: повідомлення, яке надійшло у вузол комутації, запам'ятовується в буферному запам'ятовуючому пристрої та при наявності вільного каналу зв'язку в напрямку адресата передається по цьому каналу в наступний вільний вузол. Такі вузли, які здійснюють проміжне зберігання та управління передачею повідомлень, називаються *вузлами комутації пакетів*. Коефіцієнт використання фізичних каналів зв'язку і загальна пропускна здатність вище. Однак збільшується час доставки пакетів.

Описаний приклад фактично відноситься до випадку, який передбачає незалежну маршрутизацію кожного пакету. Такий режим роботи називається дейтаграмним, і при його використанні комутатор може змінити маршрут якого-небудь пакету в залежності від стану мережі – працездатності каналів та інших комутаторів, довжини черг пакетів в сусідніх комутаторах і т.п. Існує й інший режим роботи – передача пакетів по віртуальному каналу, який представляє собою єдиний маршрут, який з'єднує кінцеві вузли. У свою чергу віртуальні канали можуть бути динамічними (маршрутизатори самі визначають шлях з

подальшим запам'ятовуванням і використанням) і постійні (що встановлюються вручну адміністраторами).

Під *комутацією повідомлень* розуміється передача єдиного блоку даних між транзитними комп'ютерами мережі з тимчасовою буферизацією цього блоку на диску кожного комп'ютера. Повідомлення, на відміну від пакету, має довільну довжину, яка визначається не технологічними міркуваннями, а змістом інформації, що містить повідомлення. Наприклад, повідомленням може бути текстовий документ, файл з кодом програми, електронний лист. Транзитні комп'ютери можуть з'єднуватися між собою як мережею з комутацією пакетів, так і мережею з комутацією каналів.

Мережі з комутацією повідомлень послужили прототипом сучасних мереж з комутацією пакетів і на даному етапі розвитку, в чистому вигляді, практично не існують.

Способи передачі даних по лініях зв'язку

Залежно від напрямку можливої передачі даних, способи передачі по лініям зв'язку діляться на наступні типи.

1. Симплексний – передача здійснюється по лінії зв'язку тільки в одному напрямку.

2. Напівдуплексний – передача ведеться в обох напрямках, але поперемінно в часі (приклад – технологія Ethernet в LAN).

3. Дуплексний – передача ведеться одночасно в двох напрямках.

Останній режим є найбільш універсальним та продуктивним способом роботи каналу. Найпростішим варіантом організації дуплексного режиму є використання двох незалежних фізичних каналів (двох пар провідників або двох світловодів) в кабелі, кожен з яких працює в симплексному режимі, тобто передає дані в одному напрямку. Така ідея лежить в багатьох мережевих технологіях, наприклад, в Fast Ethernet, ATM. Існують і інші варіанти організації дуплексного режиму.

Лекція 4. Технічні засоби комп’ютерних мереж

Технічні засоби визначають наступні основні характеристики мережі.

1. Продуктивність.
2. Швидкість передачі інформації.
3. Протяжність.
4. Топологію.

До технічних засобів КМ прийнято відносити канали передачі даних та різні засоби підключення комп'ютерів до середовища передачі.

В якості середовища WAN використовуються мережі передачі інформації загального призначення, зокрема телефонні, а також спеціалізовані: супутникові та оптоволоконні канали передачі.

В якості середовища передачі в LAN використовуються: коаксіальний кабель, кручені пари дротів (рос.: проводов) та оптоволоконні середовища.

В LAN використовуються коаксіальні кабелі з різним хвильовим опором від 50 до 120 Ом. Однак частіше застосовують з 50 Ом. Для досягнення максимального рівня сигналу, розмір сегменту коаксіального кабелю повинен бути кратний довжині хвилі сигналу, що передається.

Кабелі на скрученій, або крученій парі (Twisted Pair cable або TP), на відміну від коаксіального кабелю, симетричні і використовуються для диференціальної (балансної) передачі сигналу. Звідси походить інша назва цих кабелів – симетричні (balanced cable), під яке підпадають кабелі з четвірок дротів. Іноді ця назва перекладається як «збалансовані». На даний час в LAN кабелі на базі кручених пар є найбільш поширеними.

Подібне середовище передачі використовується в технологіях 10Base-T, 100Base-T, 1000Base-T, Token Ring, 100VG-AnyLAN та ін. Кабелі можуть містити 4 пари провідників або являти собою джгути з 25 і більше пар неекранованих (UTP – Unshielded twisted pair) або екранованих (STP – Shielded twisted pair) проводів. Існують також їх різновиди – фольгована віта пара (FTP – Foiled TP), фольгована екранована кручена пара (S/FTP), незахищена екранована кручена пара (U/STP), захищена екранована кручена пара (SF/UTP). Неекрановані дроти, як правило, мають хвильовий опір в 100 Ом +/- 15%, а екрановані – 150 Ом +/- 15%. Кожен тип кабелю, в свою чергу, може ставитися до однієї з декількох категорій (CAT1 – CAT7). Основна відмінність між категоріями полягає в частотних характеристиках (таблиця 4.1).

Таблиця 4.1

Категорія крученої пари, смуги частот та призначення

Категорія	*Смуга частот (рос.: полоса частот), МГц*	*Застосування*	*Примітка*
CAT1	0,1	Телефоні лінії	Модемне з'єднання
CAT2	1	Телефоні лінії, Token Ring, Arcnet	До 4 МБит/с
CAT3	16	Телефоні лінії, Token Ring, 10BASE-T, 100BASE-T4	До 10 Мбит/с (до 100 в 100BASE-T4 <100 м)
CAT4	20	Token Ring, 10BASE-T, 100BASE-T4	До 16 Мбит/с (по одній парі)
CAT5	100	Телефоні лінії, 100Base-T	До 100 МБит/с (при двох парах)
CAT5e	100	100BASE-T, 1000BASE-T	До 100 МБит/с (при двох парах), До 1ГБит/с (при 4-х парах)
CAT6	250	10GBASE-T	До 10 Гбит/с (до 55 м)
CAT6a	500	10GBASE-T	До 10 Гбит/с (до 100 м)
CAT7	600	10GBASE-T	До 10 Гбит/с
CAT7a	до 1200	40GbE, 100GbE	До 40 Гбит/с (до 50 м) До 100 Гбит/с (до 15 м)

Залежно від категорії кабелю визначається максимально допустима довжина сегмента кабелю між двома активними пристроями, наприклад, PC та концентратором. Наприклад, для технології 100BASE-T довжина сегмента кабелю не повинна перевищувати 100 м.

Для кабелю на основі кручених пар (рис. 4.1) в основному використовуються мідні провідники діаметром 0,51 +/- 0,01 мм (калібр 24 AWG), 0,404 мм (калібр 26 AWG), 0,643 мм (калібр 28 AWG).

Рис. 4.1. Приклад маркування TP-кабелю

Для підключення кручених пар проводів використовується уніфікований роз'єм 8P8C (помилково званий RJ-45), що має 8 контактів і фіксатор.

Асоціація телекомунікаційної промисловості США (TIA) підготувала ряд стандартів, що визначають в тому числі і розподіл контактів при прямому і перехресному з'єднаннях кабелів в мережах Ethernet (рис. 4.2, 4.3).

Призначення контактів, наприклад, в 10BASE-T:

1 – TX+ – прямий сигнал передачі;

2 – TX- – інверсний сигнал передачі;

3 – RX+ – прямий сигнал прийому;

6 – RX- – інверсний сигнал прийому.

Medium Dependent Interface (MDI) – порт Ethernet абонентського пристрою (наприклад, мережевого адаптера PC). Контакти 1 та 2 використовуються для передачі (Tx) інформації, 3 та 6 – для прийому (Rx).

Medium Dependent Interface with Crossover (MDI-X, MDIX) – Ethernet-інтерфейс, який використовується в концентраторах та комутаторах. Контакти 1 та 2 використовуються для прийому (Rx) інформації, 3 та 6 – для передачі (Tx).

Для з'єднання MDI-MDIX використовується прямий кабель, для MDI-MDI (MDIX-MDIX) – кроссоверний (кроссірованний) кабель.

Примітка: існують концентратори/комутатори, що мають порти для перехресного з'єднання і їх маркують, як X. Крім того, деякі виробники мережевого обладнання використовують позначення MPR та DTE для, відповідно, MDI та MDI-X.

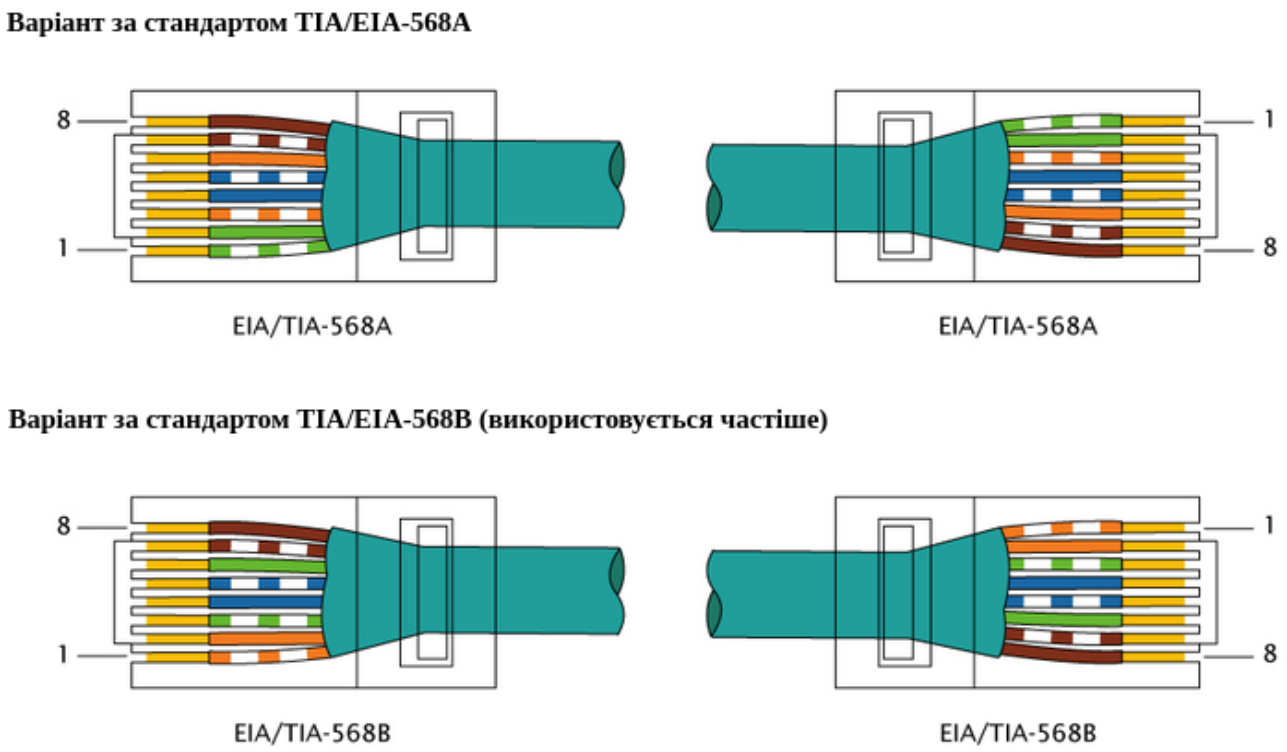

Рис. 4.2. Пряме з'єднання (з'єднання комп'ютер-концентратор/комутатор)

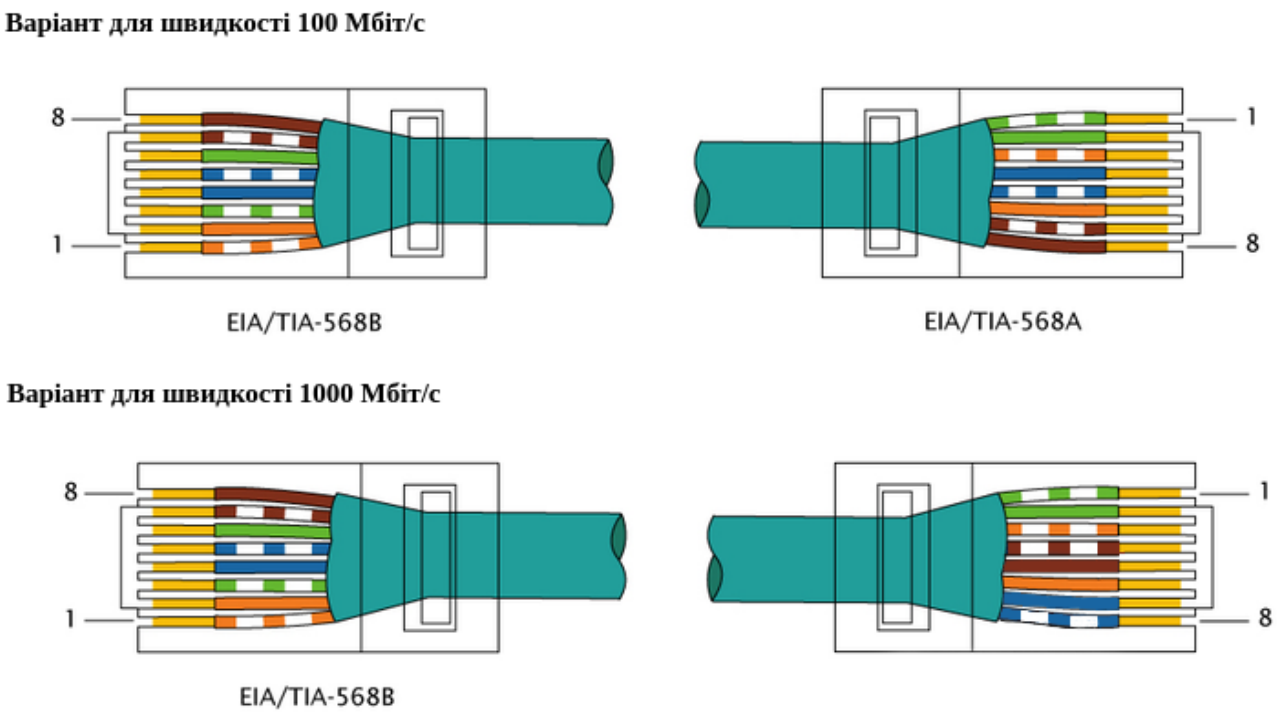

Рис. 4.3. Перехресне з'єднання (з'єднання комп'ютер-комп'ютер)

Найбільш перспективним передавальним середовищем, що забезпечує швидкість передачі в декілька Гбіт/с є оптоволоконний кабель. В якості середовища в ньому використовується оптичне волокно (світловод), що представляє собою тонку скляну нитку товщиною 50–100 мкм. Таке середовище несприйнятливе до електричних перешкод та дозволяє передавати сигнал на 10 км. Такі кабелі можуть бути одно- та багатомодовими, складатися з однієї жили (симплексні), двох волокон (дуплексні) та багатожильні (від 4 до декількох сотень волокон). Діаметр волокон та робоча частота впливають для затухання сигналу та відстань використання.

Зокрема оптоволоконні середовища передачі використовуються в стандартах Ethernet для формування стекових рішень або для передачі на великі відстані.

Приклади сучасних стандартів Gigabit Ethernet представлені в таблиці 4.2.

Відомими є також 10-гігабітний (10GBASE-сстандарти), 40-гігабітний (40Gbe) та 100-гігабітний (100Gbe) Ethernet. Більш детально дивитися за адресами:

https://en.wikipedia.org/wiki/10_Gigabit_Ethernet

https://en.wikipedia.org/wiki/100_Gigabit_Ethernet

Слід зазначити, що оптоволоконні кабелі окрім того, що працюють на різних частотах, мають різні наповнювачі (буфери), різні за складом, профілем, наповнювачем, різними температурними характеристиками. Температура експлуатації дуже важлива для подібних середовищ передачі.

Таблиця 4.2

Поширені сучасні стандарти Gigabit Ethernet

Назва	*Середа передачі*	*Відстань*
1000BASE-CX	Збалансований мідний кабель	25 метрів
1000BASE-SX	Багатомодове волокно	550 метрів
1000BASE-LX	Одномодове волокно	5км
1000BASE-SX	Багатомодове волокно використовується 850nm довжина хвилі	550 метрів
1000BASE-LH	Одномодове або багатомодове волокно використовується 1310nm довжина хвилі	10км
1000BASE-ZX	Одномодове волокно на 1550nm довжина хвилі	~ 70км
1000BASE-LX10	Одномодове волокно використовується 1310nm довжина хвилі	10км
1000BASE-BX10	Одномодове волокно, по single-strand fiber: 1490nm прямий канал 1310nm зворотний канал	10км
1000BASE-T	Віта пара (CAT-5, CAT-5e, CAT-6, CAT-7)	100 метрів
1000BASE-TX	Віта пара (CAT-6, CAT-7)	100 метрів

Підключення РС до передавального середовища здійснюється за допомогою спеціальних пристроїв – *мережевих контролерів* (адаптерів). З їх допомогою створюються КМ простої конфігурації – лінійної або кільцевої. Для побудови більш складних топологій мереж використовуються додаткові засоби мережі: повторювачі, мости, маршрутизатори та шлюзи.

Повторювачем (Repeaters) називається пристрій, що здійснює узгодження електричних параметрів сполучених мереж і зазвичай застосовується в LAN для збільшення довжини сегментів. Повторювачі «прозорі», тобто інші пристрої (РС, маршрутизатори, та т.ін.) не здатні виявити їх присутності.

Концентратор (Concentrator, HUB) – в LAN з топологією типу зірка пристрій з єдиною шиною, який об'єднує комп'ютери в мережу. У мережі Ethernet це багатопортовий повторювач. У мережах з топологією кільця (Token Ring, FDDI) він виконує функції комутатора, забезпечуючи цілісність кільця, навіть якщо деякі вузли відключені.

Концентратор завжди змінює фізичну топологію мережі, але при цьому залишає без зміни її логічну топологію.

Трафік (потік) – повний інформаційний потік в комунікаційній системі.

Поширення трафіку, призначеного для комп'ютерів деякого сегменту мережі тільки в межах цього сегменту, називається *локалізацією трафіку*.

Логічна структуризація мережі – процес розбиття мережі на сегменти з локалізованим трафіком.

Міст (Bridge) – ділить середу передачі мережі на частини (часто званими логічними сегментами, рис. 4.4), передаючи інформацію з одного сегменту в інший тільки в тому випадку, якщо така передача дійсно необхідна, тобто якщо адреса PC призначення належить іншій підмережі. Тим самим міст ізолює трафік однієї підмережі від трафіку іншої, підвищуючи загальну продуктивність передачі даних в мережі. Локалізація трафіку не тільки економить пропускну здатність, але і зменшує можливість несанкційованого доступу до даних, тому що кадри не виходять за межі свого сегмента і їх складніше перехопити зловмиснику.

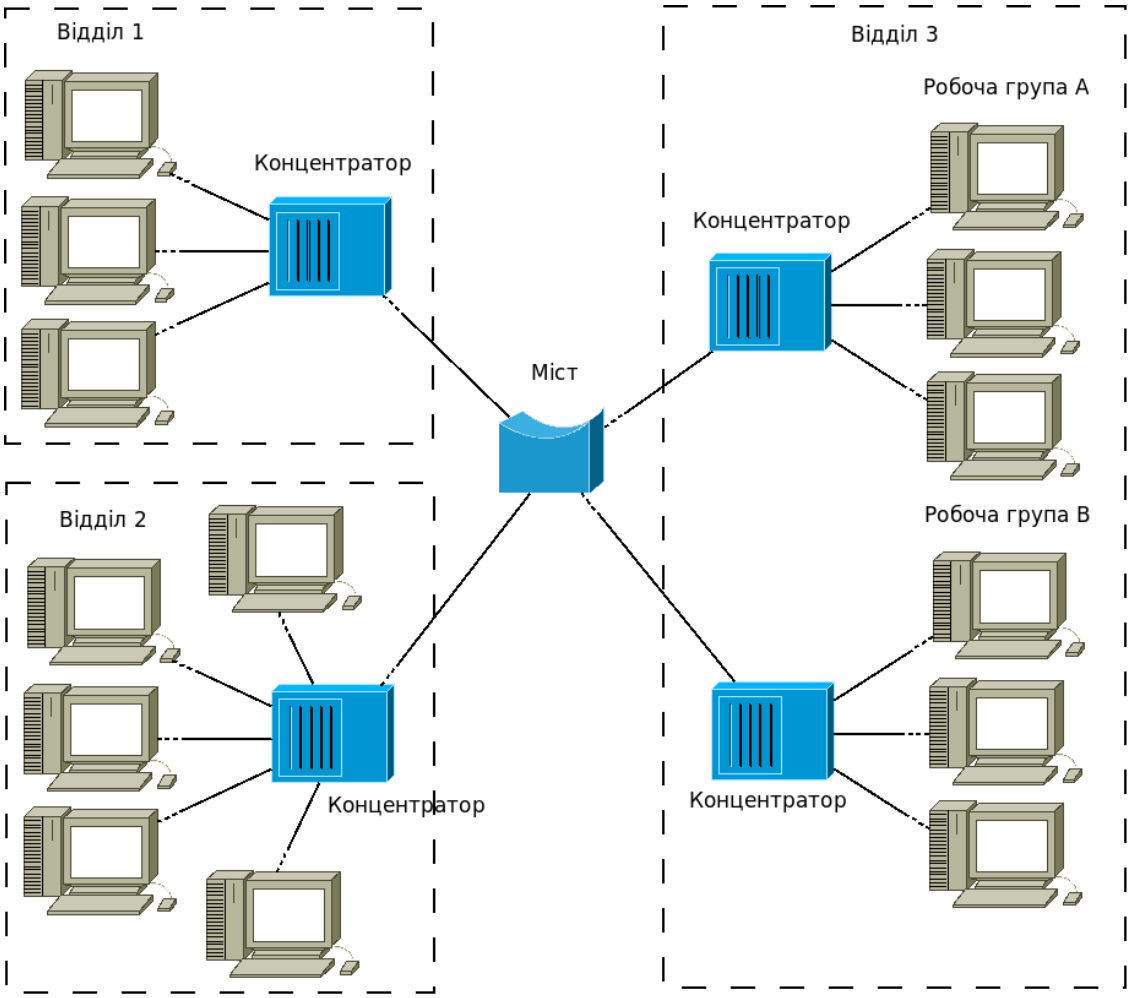

Рис. 4.4. Логічна структуризація мережі за допомогою моста

Мости використовують для локалізації трафіку *апаратні адреси* (MAC-адреси) мережевих адаптерів. Це ускладнює розпізнавання приналежності PC до певного логічного сегменту, оскільки сам адрес не містить ніякої інформації про це. Тому міст досить спрощено представляє розподіл мережі на сегменти – він запам'ятовує через який порт на нього поступив кадр даних від кожного комп'ютера мережі, і, в подальшому, передає кадри, призначені для цього комп'ютера на цей порт. Точної топології зв'язків між логічними сегментами міст не знає. Через це застосування мостів призводить до значних обмежень на конфігурацію зв'язків мережі – сегменти повинні бути з'єднані таким чином, щоб в мережі не утворювалися замкнуті контури.

Комутатор (Switch, Switching Hub) – за принципом обробки кадрів нічим не відрізняється від моста. Основна його відмінність від моста в тому, що він є свого роду комунікаційним мультипроцесором, тому що кожен його порт оснащений спеціалізованим процесором, який обробляє кадри по алгоритму моста незалежно від процесорів інших портів (тобто комутатори обробляють кадри в паралельному режимі). За рахунок цього загальна продуктивність комутатора набагато вище продуктивності звичайного моста, що має однопроцесорний блок – комутатори можуть передавати до декількох мільйонів кадрів в секунду, в той час як мости зазвичай обробляють 3-5 тисяч кадрів в секунду.

Комутатор називають неблокуючим, якщо він може передавати кадри через свої порти з тією ж швидкістю, з якою вони на них надходять.

Багато моделей комутаторів дозволяють адміністраторам задавати умови фільтрації кадрів.

Для прискорення операцій комутації все сучасні комутатори використовують замовні спеціалізовані BIC (великі інтегральні схеми) – ASIC, оптимізовані для виконання основних операцій комутації.

ASIC – високошвидкісна спеціалізована інтегральна схема, що забезпечує продуктивність комутації у деяких пристроях більше 1 мільярду пакетів в секунду (містить на кристалі процесор, блок пам'яті та інші блоки).

Значення максимального числа MAC-адрес, яке може запам'ятати процесор порту комутатора, залежить від його області застосування. Комутатори робочих груп зазвичай підтримують лише кілька адрес на порт. Комутатори відділів підтримують кілька сотень адрес, а комутатори магістралей мереж – від декількох тисяч (зазвичай 4000-8000 адрес) до декількох сотень тисяч.

Приклади високошвидкісних комутаторів з підтримкою маршрутизації:

– *HPE FlexFabric 11900 Switch Series* (2013) – підтримує масштабування до 384 1/10 гігабітних портів та до 64 40-гігабітних портів, швидкість комутації до 7.7 Тбіт/с, 5.76 млрд. пакетів в секунду (64-байтні пакети), кількість записів MAC-адрес: 131072.

– *HPE FlexFabric 12900E Switch Series* (2016) – рішення для підтримки віртуалізації центрів обробки даних (ЦОД) з ядром нового покоління, підтримує

до768 портів 40Gbe, до 768 портів 10Gbe, до 576 портів 100Gbe та ін., в залежності від конфігурації може забезпечити продуктивність комутації до 184 Тбіт/с, пропускна здатність до 92.1 млрд. пакетів в секунду.

Маршрутизатор (Routers) – більш ефективно і більш надійно, ніж мости, ізолює трафік окремих частин мережі один від одного. Маршрутизатор утворюють логічні сегменти за допомогою явної адресації, тому що використовують не плоскі апаратні, а *складові числові адреси*. У цих адресах є поле номера мережі, так що всі PC, у яких значення цього поля однакове, належать до одного сегмента, який називається підмережею (subnet). Крім локалізації трафіку маршрутизатори можуть працювати в мережі із замкнутими контурами. При цьому вони здійснюють вибір найбільш раціонального маршруту з декількох можливих. Іншою функцією маршрутизаторів є їх здатність зв'язувати в єдину мережу підмережі, побудовані з використанням різних мережевих технологій (наприклад, Ethernet та 3G).

Крім перерахованих пристроїв окремі частини мережі може з'єднувати *шлюз* (gateway). Зазвичай основною причиною, по якій його використовують в мережі, є необхідність об'єднати мережі з різними типами системного та прикладного ПЗ, а не бажання локалізувати трафік. Проте шлюз забезпечує і локалізацію трафіку як деякий побічний ефект.

Лекція 5. Адресація комп’ютерів в комп’ютерних мережах. Загальні положення

До адреси вузла мережі та схеми його призначення можна пред'явити кілька вимог.

1. Адреса повинна унікально ідентифікувати PC в мережі будь-якого масштабу.

2. Схема призначення адрес повинна зводити до мінімуму ручну працю адміністратора та ймовірність дублювання адрес.

3. Адреса повинна мати ієрархічну структуру, зручну для побудови великих мереж.

4. Адреса повинна бути зручною для користувачів мережі, тобто вона повинна мати символьне уявлення.

5. Адреса повинна мати компактне представлення, щоб не перевантажувати пам'ять комунікаційної апаратури.

Оскільки всі ці вимоги важко поєднати в рамках якої-небудь однієї схеми адресації, то на практиці використовується відразу кілька схем, так, що вузол має одночасно кілька адрес-імен. Кожна адреса використовується в тій ситуації, коли відповідний вид адресації найбільш зручний. А щоб не виникало плутанини та PC завжди однозначно визначалася своєю адресою, використовуються спеціальні допоміжні протоколи, які за адресою одного типу можуть визначити адреси інших типів.

Найбільшого поширення набули три схеми адресації вузлів.

1. *Апаратні (Hardware) адреси*. Призначені для мережі невеликого або середнього розміру, тому вони не мають ієрархічної структури. Типовим представником є адреса мережевого адаптера локальної мережі (MAC-адреса). Вона зазвичай використовується тільки апаратурою, тому її роблять по можливості компактною (наприклад, 0081005e24a8). Ця електронна адреса записується в адаптер при його виготовленні.

2. *Символьні адреси або імена*. Призначені для запам'ятовування людьми і тому несуть смислове навантаження. Такі адреси легко використовувати в мережах різного масштабу. Для роботи у великих мережах символьне ім'я може мати складну ієрархічну структуру (наприклад: ftp1-arch1.ucl.ac.uk).

3. *Числові складені адреси* (рос.: числовые составные адреса). Символьні імена зручні для людей, але через змінний формат та потенційно велику довжину їх передача по мережі не економічна. Тому для роботи у великих мережах в якості адрес вузлів використовують числові складені адреси фіксованого та компактного форматів. Типовими представниками є IP та IPX-адреси. У них підтримується дворівнева ієрархія: адреса ділиться на старшу частину (номер мережі) та молодшу (номер вузла). Такий поділ дозволяє передавати

повідомлення між мережами тільки на підставі номера мережі, а номер вузла використовується тільки після доставки повідомлення в потрібну мережу.

Останнім часом, щоб зробити маршрутизацію у великих мережах ефективнішою, пропонуються складніші варіанти числової складовою адресації, відповідно до якої адреса має три і більше складових. Такий підхід, зокрема, реалізований у версії протоколу IPv6, призначеного для роботи в мережі Internet.

Проблема встановлення відповідності між адресами різних типів, якою займається служба дозволу імен, може вирішуватися як повністю централізованими, так і розподіленими засобами. У разі централізованого підходу в мережі виділяється один комп'ютер (сервер імен), в якому зберігається таблиця відповідності одна одній імен різних типів. Всі інші комп'ютери звертаються до нього. При другому підході кожна РС сама вирішує завдання встановлення відповідності між іменами. Недолік – широкомовний режим надсилання повідомлення. У великих мережах він практично не реалізований і використовується перший підхід (наприклад, служба Domain Name System – DNS).

Лекція 6. Модель взаємодії відкритих систем (модель OSI – Open System Interconnection)

Архітектура мережі має на увазі уявлення мережі у вигляді системи елементів, кожен з яких виконує певну приватну функцію, при цьому всі елементи разом узгоджено вирішують загальну задачу взаємодії комп'ютерів. Тобто архітектура мережі відбиває декомпозицію загальної задачі взаємодії комп'ютерів на окремі підзадачі, які повинні вирішуватися окремими елементами мережі. Одним з важливих елементів архітектури мережі є комунікаційний протокол – формалізований набір правил взаємодії вузлів мережі.

На даний час використовується велика кількість мережевих протоколів, причому в рамках однієї мережі визначається відразу декілька з них. Прагнення до максимального впорядкування та спрощення процесів розробки, модернізації та розширення мереж визначило необхідність введення стандартів, що регламентують принципи та процедури організації й взаємодії абонентів КМ. З цією метою з 1977 по 1984 рік ряд міжнародних організацій по стандартизації – ISO, ITU-T та ін., розробили модель, яка зіграла значну роль в розвитку мереж. Вона називається еталонною моделлю взаємодії відкритих систем (Open System Interconnection – OSI) – рис. 6.1. Повний опис цієї моделі займає більше 1000 сторінок тексту.

Кожен рівень моделі OSI має справу з одним певним аспектом взаємодії мережевих пристроїв. Модель OSI описує тільки системні засоби взаємодії, реалізовані ОС, системними утилітами, системними апаратними засобами. Модель не включає засоби взаємодії додатків кінцевих користувачів. Свої власні протоколи взаємодії додатку реалізовують, звертаючись до системних засобів – прикладним програмним інтерфейсам (API – Application Programming Interface). Таким чином, необхідно розрізняти рівень взаємодії програм та прикладний рівень. Однак, часто на практиці, програми беруть на себе функції деяких верхніх рівнів моделі OSI.

Нехай додаток звертається із запитом до прикладного рівня, наприклад, до файлової служби. На підставі цього запиту ПЗ прикладного рівня формує повідомлення стандартного формату. Звичайне повідомлення складається із заголовку та поля даних. Заголовок містить службову інформацію, яку необхідно передати через мережу прикладному рівню машини адресата, щоб повідомити йому яку роботу треба виконати. Поле даних повідомлення може бути порожнім або містити будь-які дані. Після формування повідомлення, прикладний рівень направляє його вниз по стеку на рівень представлення. Протокол рівня представлення, на підставі інформації отриманої із заголовка

прикладного рівня, виконує необхідні дії та додає до повідомлення власну службову інформацію – заголовок свого рівня, в якому містяться вказівки для протоколу цього рівня машини адресата і т.д.

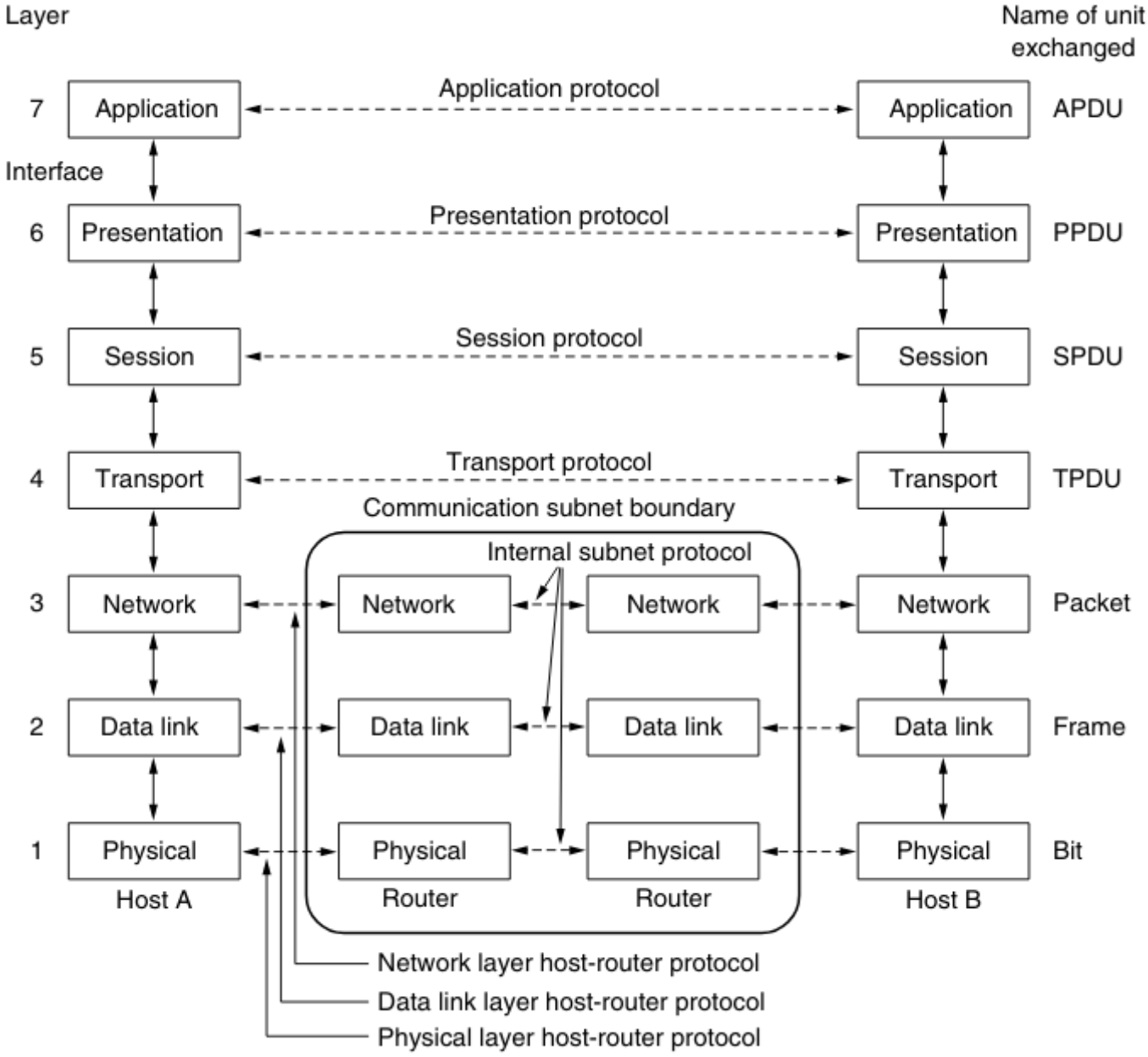

Рис. 6.1. Модель взаємодії відкритих систем ISO/OSI[1]
(International Standards Organization / Open System Interconnection)

Деякі реалізації протоколів розміщують службову інформацію не тільки на початку повідомлення у вигляді заголовка, але і у кінці у вигляді так званого «кінцевіка».

1 Рисунок взятий з книжки Andrew S. Tanenbaum, David J. Wetherall. Computer Networks, 5th Edition. – Prentice Hall, Indian International Ed., 2010. – 960 p. ISBN-10: 9332518742, ISBN-13: 978-8131770221.

Досягнувши фізичного рівня повідомлення передається по лініях зв'язку. Коли повідомлення по мережі поступає на машину-адресат, воно приймається її фізичним рівнем і послідовно переміщається вгору з рівня на рівень. Кожен рівень аналізує і обробляє заголовок свого рівня, виконуючи відповідні даному рівню функції, а потім видаляє цей заголовок і передає повідомлення на рівень вище.

Поряд з терміном «*повідомлення*» (*message*) існують і інші терміни. У стандартах ISO для позначення одиниць даних, з якими мають справу протоколи різних рівнів, використовується загальна назва – протокольний блок даних (Protocol Data Unit, PDU). Для позначення блоків даних певних рівнів часто використовуються спецназви: кадр (frame), пакет (packet), дейтаграма (datagram), сегмент (segment).

У моделі OSI розрізняють два основних типи протоколів: з встановленням з'єднання (connection-oriented) та без попереднього встановлення з'єднання (connectionless) або дейтаграмні протоколи.

У протоколах з встановленням з'єднання перед обміном даними відправник та одержувач повинні спочатку встановити з'єднання і, можливо, вибрати деякі параметри протоколу, які вони будуть використовувати при обміні даними. Після завершення діалогу вони повинні розірвати це з'єднання.

У протоколах другого типу відправник просто передає повідомлення коли воно готове.

При взаємодії РС використовуються протоколи обох типів.

Фізичний рівень (Physical layer)

Даний рівень має справу з передачею бітів по фізичним каналам зв'язку. До цього рівня мають відношення характеристики фізичних середовищ передачі даних (смуга пропускання, перешкодозахищеність, хвильовий опір і ін.). На цьому ж рівні визначаються характеристики електричних сигналів, що передають дискретну інформацію. Крім того, тут стандартизуються типи роз'ємів і призначення кожного контакту.

Функції фізичного рівня реалізуються у всіх пристроях, підключених до мережі. З боку РС ці функції виконуються мережним адаптером або послідовним портом.

Канальний рівень (Data link layer)

До завдань цього рівня входять перевірка доступності середовища передачі, а також реалізація механізмів виявлення та корекції помилок. Якщо на фізичному рівні просто пересилаються біти, то на цьому рівні біти групуються в набори, так звані кадри (frames). Канальний рівень забезпечує коректність

передачі кожного кадру, вміщуючи спеціальну послідовність біт в початок і кінець кожного кадру, для його виділення, а також обчислює контрольну суму, обробляючи всі байти кадру певним способом і додаючи контрольну суму до кадру. Цей рівень може не тільки виявити помилки, але і виправляти їх за рахунок повторної передачі пошкоджених кадрів. Однак функція виправлення помилок для нього не є обов'язковою.

В LAN протоколи канального рівня використовуються РС-ми (мережеві адаптери та їх драйвери), мостами, комутаторами і маршрутизаторами. У WAN функції цього рівня часто поєднуються з функціями мережевого рівня.

В цілому рівень являє собою потужний і закінчений набір функцій з пересилання повідомлень між вузлами мережі. У деяких випадках протоколи рівня виявляються самодостатніми транспортними засобами і можуть допускати роботу понад них безпосередньо протоколів прикладного рівня або програм, без залучення коштів мережевого і транспортного рівнів.

Найвідомішими стандартами, що регламентують роботу LAN та MAN на канальному та фізичному рівнях, є велика група стандартів IEEE 802. Згідно цих стандартів канальний рівень поділяється на два підрівня: MAC (Media Access Control) та LLC (Logical Link Control). Поле даних кадру LLC (в LLC всього 4-ри поля та спеціальні біти прапорців) призначене для передачі по мережі пакетів протоколів верхніх рівнів (наприклад: IP, IPX та ін.).

Мережевий рівень (Network layer)

Служить для утворення єдиної транспортної системи, що об'єднує декілька мереж. Ці мережі можуть використовувати абсолютно різні принципи передачі повідомлень між кінцевими вузлами і володіти довільною структурою зв'язків. Рівень призначений для забезпечення маршрутизації інформації (основна функція рівня) і управління мережею передачі даних. На відміну від канального рівня, що має справу з фізичними адресами, мережевий рівень працює з логічними адресами – числовими складовими.

Рівень надає транспортному рівню послуги з встановленням логічного з'єднання (наприклад, в разі X.25) або без встановлення такого (наприклад, IP – Internet Protocol).

До відомих протоколів мережного рівня належать: IP, ICMP (Internet Control Message Protocol) стека протоколів TCP/IP, а також протокол міжмережевого обміну пакетами IPX (Internet Packet Exchange) стека Novell. Протоколи рівня, що відповідають за відображення адреси вузла, яка використовується на цьому рівні, в локальну адресу мережі (MAC-адресу), називають протоколами дозволу адрес. Прикладом такого протоколу, який функціонує на мережевому рівні, є ARP (Address Resolution Protocol) стека TCP/IP і має реалізації не тільки для IP.

Транспортний рівень (Transport layer)

Цей рівень забезпечує програмам або верхнім рівням стека (прикладному та сеансовому) передачу даних з тим ступенем надійності, яка їм потрібна. Модель OSI визначає 5 класів сервісу, що надається транспортним рівнем. Цей рівень повинен існувати хоча б тому, що іноді всі три нижніх рівня (фізичний, канальний та мережевий) надає оператор послуг зв'язку. Протокол рівня надає споживачеві послуг необхідну надійність.

Як правило, всі протоколи, починаючи з цього рівня і вище, реалізуються програмними засобами кінцевих вузлів мережі – компонентами їх мережевих ОС. Як приклад транспортних протоколів можна привести: TCP (Transmission Control Protocol), UDP (User Datagram Protocol), SPX стека Novell (Sequenced Packet Exchange).

Протоколи нижніх чотирьох рівнів узагальнено називають *мережевим транспортом* або *транспортною підсистемою*, тому що вони повністю вирішують задачу транспортування повідомлень із заданим рівнем якості в складених мережах з довільною топологією і різними технологіями. Решта три верхніх рівні вирішують задачі надання прикладних сервісів на основі транспортної підсистеми.

Сеансовий рівень (Session layer)

Рівень забезпечує управління діалогом: фіксує, яка зі сторін є активною в даний момент, надає засоби синхронізації. Останні дозволяють вставляти контрольні точки в довгі передачі, щоб у разі відмови можна було повернутися назад до останньої контрольної точки, а не 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 та реалізують в одному протоколі.

Рівень представлення (Presentation layer)

Рівень має справу з формою подання переданої по мережі інформації, не змінюючи при цьому її зміст. За рахунок цього рівня інформація, передана прикладним рівнем однієї системи, завжди зрозуміла прикладному рівню іншої системи. За допомогою засобів даного рівня протоколи прикладних рівнів можуть подолати синтаксичні відмінності в представленні даних або ж відмінності в кодах символів, наприклад, UTF-8 та KOI8.

На цьому рівні може здійснюватися шифрування та дешифрування даних, завдяки якому секретність обміну даними забезпечується відразу для всіх

прикладних служб. Прикладом протоколу рівня представлення є SSL (Secure Socket Layer), що забезпечує секретний обмін повідомленнями для протоколів прикладного рівня стека TCP/IP.

Прикладний рівень (Application layer)

Цей рівень в дійсності є набором різноманітних протоколів, за допомогою яких користувачі мережі отримують доступ до ресурсів, що розділяються, таким як: файли, принтери або Web-сторінки, а також організують свою спільну роботу, наприклад, за допомогою протоколу електронної пошти.

Одиниця даних, якою оперує цей рівень, зазвичай називаються *повідомленням* (*message*).

Найбільш поширені реалізації файлових служб прикладного рівня: SMB в MS Windows, NCP в ОС Novell Network, NFS, FTP, TFTP, що входять в стек TCP/IP.

Фізичний, канальний та мережевий – є мережезалежними, тобто протоколи цих рівнів тісно пов'язані з технічною реалізацією мережі і комунікаційним обладнанням.

Сеансовий, представлення та прикладний – орієнтовані на програми і мало залежать від технологічних особливостей побудови мережі. На протоколи цих рівнів не впливають які б то не було зміни в топології мережі, заміна обладнання або перехід на іншу мережеву технологію.

Транспортний рівень є проміжним і приховує всі деталі функціонування нижніх рівнів від верхніх. Це дозволяє розробляти програми, які не залежать від технічних засобів безпосереднього транспортування повідомлень.

Технічні комунікаційні засоби в залежності від типу можуть працювати або тільки на фізичному рівні (повторювач), або на фізичному та канальному (міст, комутатор), або на фізичному, канальному та мережевому, іноді захоплюючи й транспортний рівень (маршрутизатор).

Модель OSI представляє, хоча і дуже важливу, але тільки одну з багатьох моделей комунікацій. Ці моделі та пов'язані з ними стеки протоколів можуть відрізнятися кількістю рівнів, їх функціями, форматами повідомлень, службами, що підтримуються на верхніх рівнях, та іншими параметрами.

Лекція 7. Стек комунікаційних протоколів TCP/IP

Найважливішим напрямком стандартизації в області обчислювальних мереж є стандартизація комунікаційних протоколів. На даний час в мережах використовується велика кількість стеків комунікаційних протоколів. Найбільш відомими є стеки: TCP/IP, IPX/SPX, NetBIOS/SMB, DECnet, SNA та OSI. Всі ці стеки, крім SNA, на нижніх рівнях – фізичному і канальному, – використовують одні і ті ж добре стандартизовані протоколи Ethernet, Token Ring, FDDI і деякі інші, які дозволяють використовувати у всіх мережах одну і ту ж апаратуру. Зате на верхніх рівнях всі стеки працюють за своїми власними протоколами. Ці протоколи часто не відповідають рекомендованому моделі OSI розбиттю на рівні.

Примітка: модель OSI і стек OSI – це абсолютно різні поняття.

Стек TCP/IP був розроблений з ініціативи Міноборони США для зв'язку експериментальної мережі ARPAnet з іншими мережами, як набір загальних протоколів для різнорідного обчислювального середовища. Перші офіційні документи по протоколам IP та TCP датовані 1981 роком (RFC 791 та RFC 793 відповідно:

https://www.ietf.org/rfc.html
https://tools.ietf.org/html/rfc791
https://tools.ietf.org/html/rfc793

На даний момент найпоширеніший.

RFC (Request For Comments, робоча пропозиція, теми для обговорення) – пронумеровані серії інформаційних документів Internet, що містять технічні специфікації та стандарти, які широко використовуються в Internet.

Багаторівнева структура стека TCP/IP

Рівень I	Прикладний рівень
Рівень II	Основний (транспортний) рівень
Рівень III	Рівень міжмережевої взаємодії
Рівень IV	Рівень мережевих інтерфейсів

Рівень міжмережевої взаємодії

Цей рівень є основою всієї архітектури. Він реалізує концепцію передачі пакетів в режимі без встановлення з'єднань, тобто дейтаграмним способом. Дейтаграма – загальна назва для одиниць даних, якими оперують протоколи без встановлення з'єднань. Саме 3-й рівень забезпечує можливість переміщення пакетів по мережі, використовуючи той маршрут, який в даний момент є найбільш раціональним. Цей рівень також називають рівнем Internet, вказуючи тим самим на основну його функцію – передачу даних через складену мережу.

Основним протоколом мережевого рівня (в термінах моделі OSI) в стеку є протокол IP. IP-дейтаграма складається з IP-заголовку (рис. 7.1) та даних, які часто називають корисним навантаженням (payload). Довжина IP-заголовку нефіксована.

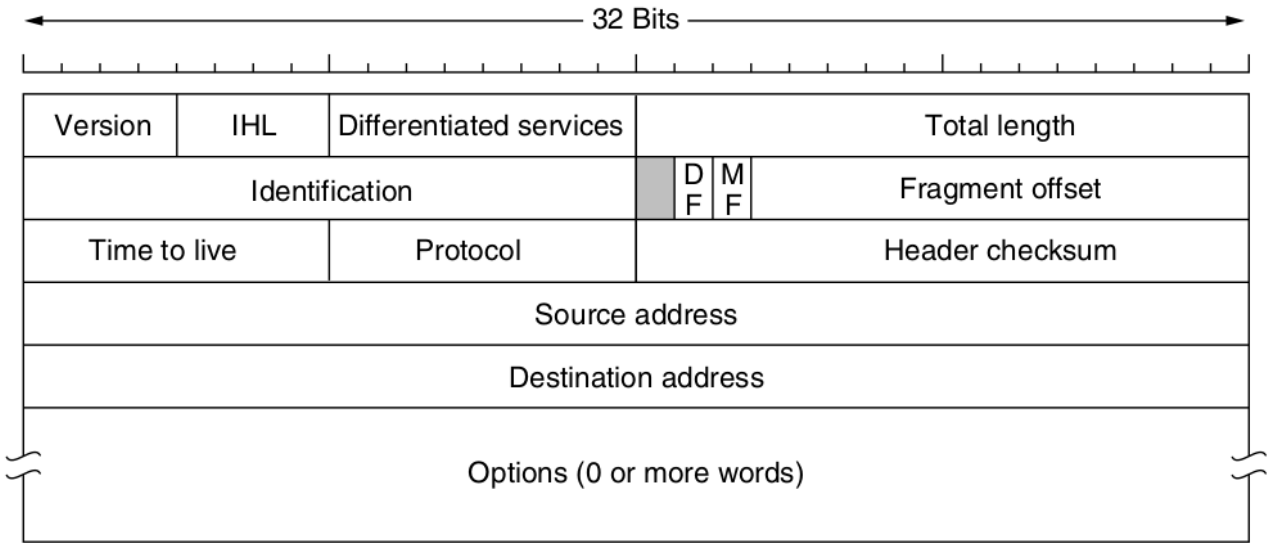

Рис. 7.1. IPv4-заголовок[2]

Поле *Версія* (Version) містить 4 для IPv4, “нова” редакція – 6 (IPv6), експериментальна – 5.

Поле *Довжина заголовка* (Internet Header Length, IHL) містить довжину IP-заголовку в 32-розрядних словах. Мінімальна довжина IP-заголовка складає 20 байт (5-ть 32-розрядних слів = 5 * 4 байт).

Поле *Тип обслуговування* (Type Of Service, TOS або Differentiated services) – в ньому вказують необхідність спеціальної обробки пакету, наприклад, мінімізації затримки, підвищення швидкості і т.д. (подробиці див. в RFC 791). В даний час більшість маршрутизаторів просто ігнорують це поле.

Поле *Довжина* (Length або Total Length) – характеризує загальну довжину в байтах IP-пакету (максимум – 65535 байт, корисного навантаження – 65515 байт). Всі хости та маршрутизатори повинні підтримувати IP-пакети довжиною

2 Рисунок взятий з книжки Andrew S. Tanenbaum, David J. Wetherall. Computer Networks, 5th Edition. – Prentice Hall, Indian International Ed., 2010. – 960 p. ISBN-10: 9332518742, ISBN-13: 978-8131770221.

не менше 576 байт (20 байт – IP-заголовок, 512 байт – корисне навантаження, 44 байта – параметри або заголовок протоколу нижнього рівня). Ця вимога гарантує, що IP-пакети такої довжини передаватимуться без фрагментації.

Поле *Ідентифікатор* (Identification) – має однакові значення у всіх фрагментах, що становлять одну IP-дейтаграму і визначається хостом-відправником.

Поле *Прапори* (Flags) – складається з 3-х біт, які керують фрагментацією.

Поле *Зсув фрагменту* (*зміщення заголовка*) (Fragment Offset) – задає місце фрагменту при складанні вихідного потоку даних. Для першого фрагменту – 0. Механізми збірки фрагментів описані в RFC 815 та 791.

Поле *Час життя* (Time To Live, TTL) – на даний час поле використовують в якості лічильника кількості вузлів (хостів, маршрутизаторів), пройдених пакетом, тобто як лічильник переходів (hop count). Кожний вузол зменшує значення поля на одиницю.

Поле *Ідентифікатор протоколу* (Protocol Identifier або Protocal) – показує, який протокол верхнього рівня вкладений в поле даних IP-пакета (значення 6 – TCP). Більш детально див. RFC 1700.

Поле *Контрольна сума* (Checksum або Header Checksum) застосовується для виявлення помилок передачі пакета.

Поле *Параметри* (Options) має змінну довжину і може взагалі бути відсутнім (див. RFC 791). Призначено в основному для управління маршрутизацією.

Поле *Вирівнювання* (Padding) – вирівнює IP-заголовок на границі 32-х-бітного слова.

Основний рівень

На цьому рівні функціонують протокол управління передачею TCP та протокол дейтаграм користувача UDP.

Протокол TCP дозволяє рівноранговим об'єктам на PC-відправника та PC-одержувача підтримувати обмін даними в дуплексному режимі. TCP поділяє потік байт на частини – сегменти, і передає їх нижчому рівню міжмережевої взаємодії. Після того як ці сегменти будуть доставлені засобами рівня міжмережевої взаємодії в пункт призначення, протокол TCP знову збере їх в безперервний потік байт.

Протокол UDP забезпечує передачу прикладних пакетів дейтаграмним способом (як і IP), і виконує тільки функції сполучної ланки (мультиплексора) між мережним протоколом і численними службами прикладного рівня або процесами користувача.

Прикладний рівень

Рівень об'єднує всі служби, що надаються системою для програм користувача. Він реалізується програмними системами, побудованими в архітектурі клієнт-сервер, що базуються на протоколах нижніх рівнів. На відміну від протоколів інших трьох рівнів, протоколи прикладного рівня займаються деталями конкретної програми і “не цікавляться” способами передачі даних по мережі.

Рівень мережевих інтерфейсів

Для кожної технології, що включається в складену мережу підмережі, повинні бути розроблені власні інтерфейсні засоби. До них відносяться протоколи інкапсуляції IP-пакетів рівня міжмережевої взаємодії в кадри локальних мережевих технологій. Наприклад, документ RFC 1042 визначає способи інкапсуляції IP-пакетів в кадри технології IEEE 802.

Найбільш відомі протоколи стека TCP/IP

Так як стек TCP/IP був розроблений до появи моделі ISO/OSI, то хоча він також має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделей OSI досить умовна (рис. 7.2).

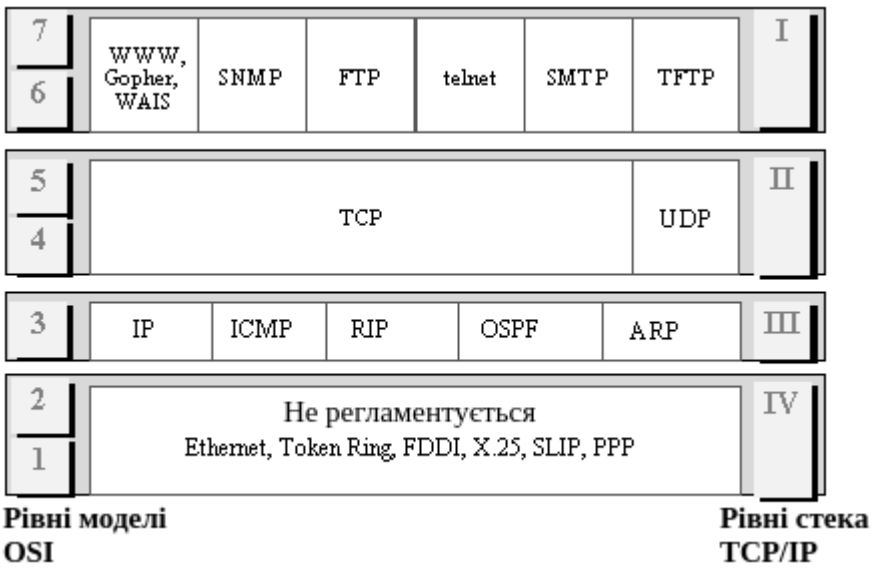

Рис. 7.2. Відповідність рівнів TCP/IP рівням моделі OSI

SLIP (Serial Line IP) – протокол, призначений для передачі пакетів IP через послідовну лінію зв'язку.

PPP (Point-to-Point Protocol, протокол "точка-точка") – швидкий та гнучкий протокол канального рівня (за моделлю OSI), призначений для передачі

через канали зв'язку типу "точка-точка" (модемні лінії зв'язку, канали ISDN) пакетів у форматі інших протоколів (наприклад, IP або IPX).

CSLIP (Compressed SLIP) – протокол для передачі пакетів IP через послідовну лінію з використанням стиснення заголовків дейтаграм TCP/IP.

ARP (Address Resolution Protocol) – використовується для визначення адрес Ethernet на підставі IP-адрес.

RIP (Routing Information Protocol) – простий протокол маршрутизації, який використовується для оновлення інформації про маршрути в рамках невеликої КМ (використовує 520-й порт UDP).

ICMP (Internet Control Message Protocol) – мережевий протокол, який використовується в мережах IP для передачі інформації про помилки, а також деяких службових повідомлень. Протокол використовують утиліти *ping* та *traceroute*.

FTP (File Transfer Protocol) – протокол передачі файлів через мережі IP. На його базі розроблена найбільш поширена мережева служба передачі файлів (використовує 21-й порт TCP для команд та 20-й порт TCP для даних).

TFTP (Trivial FTP) – простий протокол передачі файлів, що не вимагає на відміну від FTP, аутентифікації. Заснований на UDP (використовує 69 порт UDP).

SMTP (Simple Mail Transfer Protocol) – протокол передачі електронної пошти через лінії зв'язку TCP (використовує 25-й порт TCP).

POP3 (Post Office Protocol) – протокол використовується клієнтами електронної пошти для отримання електронної пошти з віддаленого сервера по TCP/IP-з'єднанню (використовує 110-й порт TCP).

IMAP (Internet Message Access Protocol) – протокол прикладного рівня для доступу до електронної пошти, який базується на TCP (143-й порт TCP).

SNMP (Simple Network Management Protocol) – простий протокол мережевого управління та адміністрування.

OSPF (Open Shortest Path First) – протокол динамічної маршрутизації, заснований на технології відстеження стану каналу, який використовує для знаходження найкоротшого шляху алгоритм Дейкстри (використовує 89-й порт IP).

TELNET (TErminaL NETwork) – протокол взаємодії користувачів між PC через текстовий інтерфейс (використовує 23-й порт TCP).

SSH (Secure SHell) – мережевий протокол прикладного рівня, що дозволяє виробляти віддалене управління ОС та тунелювання TCP-з'єднань (наприклад, для передачі файлів). SSH шифрує весь трафік, включаючи передані паролі (використовує 22-й порт TCP).

SFTP (SSH File Transfer Protocol) – протокол прикладного рівня, призначений для різних операцій з файлами поверх надійного і безпечного з'єднання.

HTTP (HyperText Transfer Protocol) – протокол прикладного рівня передачі даних. Використовує 80-й порт TCP.

IP (Internet Protocol, міжмережевий протокол) – connectionless-протокол мережевого рівня для маршрутизації, що використовується для обміну даними в мережах Internet/intranet.

TCP (Transmission Control Protocol) – connection-oriented-протокол, керуючий передачею потоку даних через IP (використовує 6-й порт IP).

UDP (User Datagram Protocol) – connectionless-протокол передачі через Internet окремих пакетів даних (використовує 17-й порт IP).

Кожний комунікаційний протокол оперує з деякою одиницею переданих даних. У стеку TCP/IP за багато років його існування утворилася така термінологія:

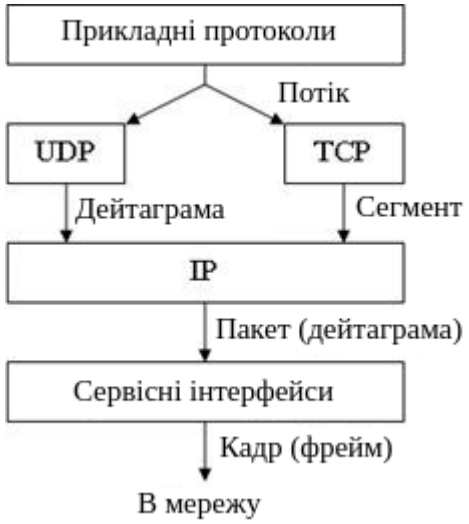

Рис. 7.3. Назва одиниць даних, що використовують в TCP/IP

Потоком називають дані, що надходять від програм на вхід протоколів транспортного рівня TCP та UDP. Протокол TCP “нарізає” з потоку даних *сегменти*. Одиницю даних протоколу UDP часто називають *дейтаграмою*. Дейтаграму протоколу IP називають також *пакетом*. У стеку TCP/IP прийнято називати *кадрами* (*фреймами*) одиниці даних протоколів, на основі яких IP-пакети переносяться через підмережі складовою мережі. При цьому не має значення, яка назва використовується для цієї одиниці даних в локальній технології.

Лекція 8. Адресація в IP-мережах

Типи адрес стеку TCP/IP

У стеці TCP/IP використовуються 3 типа адрес:
– локальні (апаратні);
– IP-адреси;
– символьні доменні імена.

Класи IP-адрес

IP-адреса 4-й версії має довжину 4-е байта (32 біта) і зазвичай записується у вигляді 4-х чисел, що представляють значення кожного байта в десятковій формі, між якими ставлять крапку. Наприклад: 128.10.2.30 – десяткова форма представлення.

10000000 00001010 00000010 00011110 – двійкова форма.

Адреса складається з двох логічних частин – номера мережі і номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка до номера вузла, визначається значеннями перших біт адреси. Значення цих біт є також ознаками того, до якого класу належить той чи інший IP-адрес. Приклад структури IP-адреси:

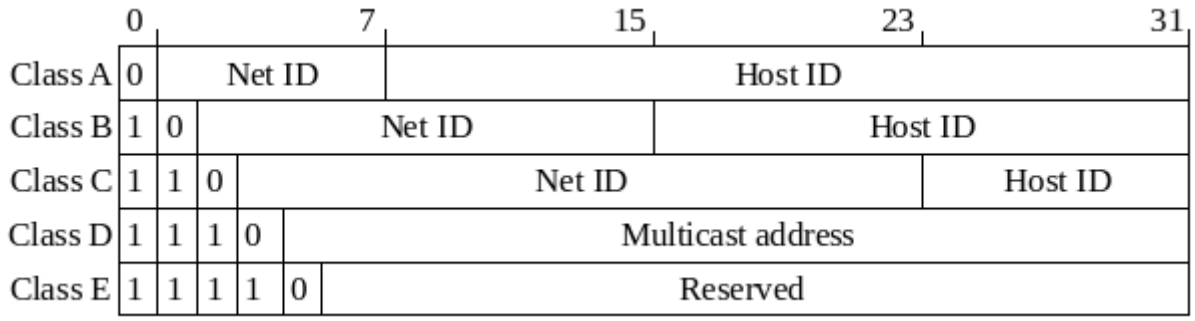

Рис. 8.1. Структура IPv4-адреси

Таблиця 8.1

Властивості адрес різних класів

Клас	*Перші біти*	*Найменший номер мережі*	*Найбільший номер мережі*	*Максимальна кількість вузлів у мережі*
A	0	1.0.0.0	126.0.0.0	2^{24}
B	10	128.0.0.0	191.255.0.0	2^{16}
C	110	192.0.1.0	223.255.255.0	2^{8}
D	1110	224.0.0.0	239.255.255.255	Multicast
E	11110	240.0.0.0	247.255.255.255	Зарезервований

Великі мережі отримують адреси класу A, середні – B, маленькі – C. Клас D позначає особливий, груповий адрес – multicast. Якщо в пакеті як адреса призначення вказана адреса класу D, то такий пакет повинні отримати всі вузли, яким визначено цю адресу. Адреси класу E зарезервовані для майбутніх застосувань.

Важливі угоди в протоколі IP

У протоколі IP існує кілька угод про особливу інтерпретацію IP-адрес.

1. Якщо весь IP-адрес складається тільки з двійкових нулів, то він позначає адресу того вузла, який згенерував цей пакет. Цей режим використовується тільки в деяких повідомленнях ICMP.

2. Якщо в поле номера мережі розташовані тільки нулі, то за замовчуванням вважається, що вузол призначення належить тій же самій мережі, що і вузол, який відправив пакет.

3. Якщо все двійкові розряди IP-адреси дорівнюють одиниці, то пакет з такою адресою призначення повинен розсилатися всім вузлам, що знаходяться в тій же мережі, що й джерело цього пакета. Така розсилка називається *обмеженим широкомовним повідомленням* (limited broadcast).

4. Якщо в поле номера вузла призначення стоять тільки одиниці, то пакет з такою адресою розсилається всім вузлам мережі із заданим номером мережі. Наприклад, пакет з адресою 192.190.21.255 доставляється всім вузлам мережі 192.190.21.0. Така розсилка називається *широкомовним повідомленням* (broadcast).

Особливий сенс має IP-адреса, перший октет якої дорівнює 127. Вона використовується для тестування програм і взаємодії процесів в межах однієї машини. Коли програма посилає дані за IP-адресою 127.0.0.1, то утворюється «петля». Ця електронна адреса має назву *loopback*. Будь-яка адреса мережі 127.0.0.0 служить для позначення свого модуля маршрутизації, а не тільки 127.0.0.1 (наприклад, 127.0.0.3).

У протоколі IP немає поняття широкомовності в тому сенсі, в якому воно використовується в протоколах канального рівня локальних мереж, коли дані повинні бути доставлені абсолютно усім вузлам. Розподіл мережі за допомогою

маршрутизаторів на частини локалізує широкомовний шторм межами однієї зі складових частин загальної мережі просто тому, що немає способу адресувати пакет одночасно всім вузлам всіх мереж складовою мережі.

Якщо деяка IP-мережа створена для роботи в «автономному режимі», без зв'язку з Internet, тоді адміністратор цієї мережі вільний призначати їй довільно обраний номер. Але і в цій ситуації для того, щоб уникнути будь-яких колізій, в стандартах Internet визначено кілька діапазонів адрес, рекомендованих для локального використання. Ці адреси не обробляються маршрутизаторами Internet ні за яких умов. Адреси, зарезервовані для локальних цілей, обрані з різних класів:

Клас А: мережа 10.0.0.0;
Клас В: діапазон з 16-ти номерів мереж 172.16.0.0. - 172.31.0.0
Клас С: діапазон з 255-ти мереж 192.168.0.0. - 192.168.255.0.

Маски

Для більш гнучкого встановлення межі між номером мережі і номером вузла, використовують маски.

Маска – це число, яке використовується в парі з IP-адресою. Двійковий запис маски містить одиниці в тих розрядах, які повинні в IP-адресі інтерпретуватися як номер мережі. Оскільки номер мережі є цілісною частиною адреси, одиниці в масці також повинні представляти безперервну послідовність.

Для стандартних класів мереж маски мають таке значення:

Клас А: 255.0.0.0
Клас В: 255.255.0.0
Клас С: 255.255.255.0

Приклад:

IP-адреса: 185.23.44.206
Маска: 255.255.255.0
Номер мережі: 185.23.44.0

У масках кількість одиниць в послідовності, що визначає межу номера мережі, не обов'язково має бути кратним 8, щоб повторювати поділ адреси на байти.

Приклад:

IP-адреса: 129.64.134.5
Маска: 255.255.128.0

Тобто:

129.64.134.5: 10000001.01000000.10000110.00000101 побітове «і»
255.255.128.0: 11111111.11111111.10000000.00000000
129.64.128.0: 10000001.01000000.10000000.00000000 ← номер мережі
0.0.6.5 ← номер вузла

IPv6

При роздачі IP-адрес в мережі Internet давно спостерігається дефіцит адрес IPv4. Дуже важко отримати адреса класу B і практично неможливо стати володарем класу A. Для пом'якшення проблеми дефіциту адрес розробники стека TCP/IP пропонують різні підходи. Принциповим рішенням є перехід на нову версію IPv6, в якій різко розширюється адресний простір за рахунок використання 16-байтних (128 біт) адрес.

8.06.2011 відбувся міжнародний день IPv6.
З кардинальних відмінностей від IPv4 слід зазначити:
– прибрані функції, які ускладнюють роботу маршрутизаторів (зокрема маршрутизатори більше не розбивають пакет на частини, хоча можлива розбивка пакету з передавальної сторони);
– прибрана контрольна сума, як надлишкова інформація;
– заголовок пакета збільшений з 20 до 40 байт;
– в надшвидкісних мережах можлива підтримка величезних пакетів до 4 Гбайт (джамбограмм);
– Time ToLive перейменовано в Hop Limit;
– з'явилося багатоадресне мовлення.
Адреси IPv6 відображаються як вісім груп по чотири шістнадцяткові цифри, розділені двокрапкою. Наприклад:

fe80:0000:0000:0000:222:15ff:fef5:f1d0

Скорочений варіант в разі повторюваних груп нулів:

fe80::222:15ff:fef5:f1d0

Додаткову інформацію про IPv6 дивиться у статі за посиланням: https://habr.com/ru/post/253803/

DHCP

Призначення IP-адрес вузлів мережі при не дуже великому розмірі мережі може представляти для адміністратора тяжку процедуру.

Протокол DHCP звільняє адміністратора від цих проблем, автоматизуючи процес призначення адрес. DHCP може підтримувати спосіб автоматичного, динамічного розподілу адрес, а так більш прості способи ручного та автоматичного статичного призначення адрес. Цей протокол працює відповідно до моделі «клієнт-сервер».

Під час старту системи комп'ютер, що є DHCP-клієнтом, посилає в мережу широкомовний запит на отримання IP-адреси. DHCP-сервер відгукується і посилає повідомлення-відповідь, що містить IP-адресу. Передбачається, що DHCP-клієнт і DHCP-сервер знаходяться в одній IP-мережі.

При динамічному розподілі адрес, DHCP-сервер видає адреса DHCP-клієнту на обмежений час, так званий *час оренди* (lease duration), що дає можливість надалі повторно використовувати цю IP-адресу для призначення іншому вузлу.

Відображення IP-адрес на локальні адреси

Однією з головних задач, які ставилися при створенні протоколу IP, є забезпечення спільної узгодженої роботи в мережі, що складається з підмереж, які в загальному випадку використовують різні мережеві технології. Безпосередньо з вирішенням цієї задачі пов'язаний рівень міжмережевих інтерфейсів стеку TCP/IP. Задача відображення IP-адресу в локальну адресу є однією з тих важливих задач, якою займається цей рівень (у термінах моделі ISO/OSI, це канальний рівень).

Для визначення локальної адреси за IP-адресою використовується протокол дозволу адреси ARP (Address Resolution Protocol). Необхідність в зверненні до цього протоколу виникає кожен раз, коли модуль IP передає пакет на рівень мережевих інтерфейсів.

Наприклад: драйвер Ethernet, IP-адреса вузла призначення відома модулю IP. Потрібно на його основі знайти MAC-адресу вузла призначення.

Для кожної мережі, підключеної до мережевого адаптера комп'ютера та до порту маршрутизатора, будується окрема ARP-таблиця. Робота ARP-протоколу починається з її перегляду. В ній міститься IP-адреса та відповідна їй MAC-адреса.

Лекція 9. Організація доменів та імен доменів. Система DNS

Організація доменів та імен доменів

Для ефективної організації іменування комп'ютерів у великих мережах, наприклад в Internet, природним є застосування ієрархічних складових імен.

У стеці TCP/IP застосовується доменна система імен, яка має ієрархічно деревоподібну структуру (рис. 9.1), що допускає використання в імені довільної кількості складових частин.

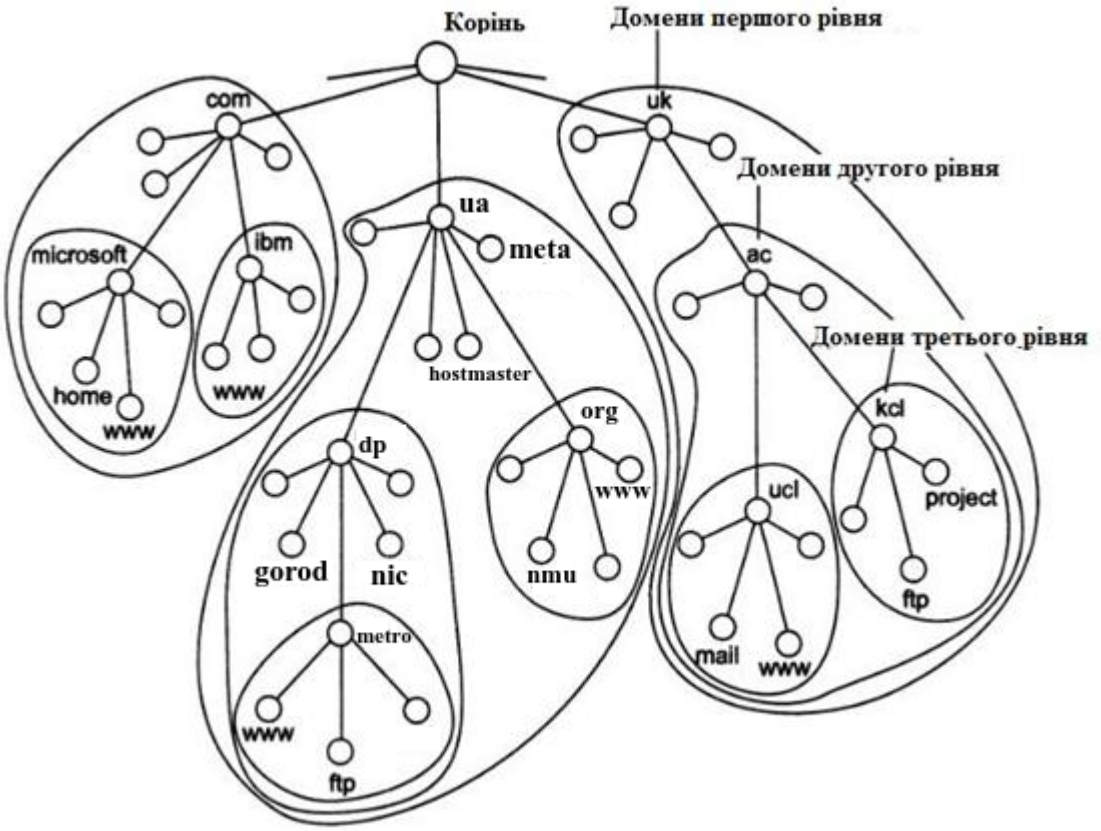

Рис. 9.1. Приклад простору доменних імен

Ієрархія доменних імен аналогічна ієрархії імен файлів, яка прийнята в багатьох файлових системах. Дерево імен починається з кореня. Запис доменного імені починається з наймолодшої складової, а закінчується найстаршою. Наприклад: www.nmu.org.ua.

Складові частини доменного імені відокремлюються один від одного крапкою.

Сукупність імен, у яких кілька старших складових частин збігаються, утворюють домен імен (domain). Наприклад, google.com та maps.google.com входять в домен com.

Примітка: термін домен дуже багатозначний, тому його потрібно трактувати в рамках певного контексту. Крім доменів імен стека TCP/IP часто згадуються домени Windows, домени колізій та інші. Загальним у всіх цих термінів є те що вони описують деяку безліч комп'ютерів, у яких є певна властивість.

Якщо один домен входить в інший домен, як його складова частина, то такий домен називають піддоменом (subdomain). Хоча назва «домен» за ним також залишається.

У доменній системі імен розрізняють короткі імена, відносні імена та повні доменні імена.

Коротке ім'я – це ім'я кінцевого вузла мережі: хосту або порту маршрутизатора.

Відносне ім'я – складене ім'я, що починається з деякого рівня ієрархії, але не з самого верхнього.

Повне доменне ім'я (fully qualified domain name, FQDN) – включає складові всіх рівнів ієрархії, починаючи з короткого імені і закінчуючи кореневою точкою: www.nmu.org.ua**.**

Необхідно підкреслити, що комп'ютери входять в домен у відповідності зі своїми складовими іменами. При цьому вони можуть мати абсолютно різні IP-адреси, які належать різним мережам та підмережам. Наприклад, в домен org.ua можуть входити хости з адресами (умовні адреси): 132.13.34.15, 61.22.100.33, 14.0.0.6.

В Internet кореневий домен раніше управляється центром InterNIC (Network Information Center). Домени верхнього рівня призначаються для кожної країни, а також на організаційній основі. Питаннями створення, підтримки і адміністративного управління доменами верхнього рівня спочатку займалася організація IANA (Internet Assigned Numbers Authority – “Адміністрація адресного простору Інтернет”), що діяла на підставі контракту з Міністерством оборони США. З часом ці питання були передані в іншу міжнародну організацію ICANN – Internet-корпорацію з присвоєння імен і номерів (Internet Corporation for Assigned Names and Numbers), а функції підрядника перейшли до Міністерства торгівлі США.

На даний час ICANN забезпечує підтримку і управління всім адресним простором DNS (Domain Name System, система доменних імен) в мережі Internet, крім TLD (top-level domain) обмеженого користування, які безпосередньо управляються американськими державними організаціями.

Технічно домени верхнього рівня доступні через систему кореневих серверів DNS, контрольовану ICANN.

ICANN заявила про відкриття вільної реєстрації доменів першого рівня для всіх інтернет-користувачів з 12 січня 2012 року.

З 2013 року компанія ICANN вже не реєструє нові доменні зони, а займається лише адмініструванням вже раніше зареєстрованих.

Офіційна інформація про діючи кореневі сервери DNS публікується на сайті Асоціації операторів Кореневих серверів DNS https://root-servers.org.

Імена доменів повинні відповідати міжнародному стандарту ISO 3166. Для позначення країн використовуються 2-х та 3-х буквені абревіатури, а для різних видів організацій – наступні позначення:

com – комерційні;
edu – освітні;
gov – урядові;
org – некомерційні;
mil – військові;
int – міжнародні;
net – підтримують мережі;
та ін.

Перші домени типу gTLD (global TLD) з'явилися в січні 1985 року. Тоді їх було тільки 7.

На 41-й конференції ICANN в 2011 році була прийнята програма New gTLD. Тепер gTLD можуть реєструвати на себе юридичні особи, зокрема комерційні компанії, представники влади будь-якого рівня і некомерційні організації.

Повний список всіх доменів верхнього рівня представлений за адресою: https://www.iana.org/domains/root/db

Система доменних імен DNS

Відповідність між доменними іменами та IP-адресами може встановлюватися як засобами локального хосту, так і засобами централізованої служби. На етапі розвитку Internet на кожному хості вручну створювався текстовий файл з ім'ям hosts. Приклад:

```
# IP FQDN Aliases
127.0.0.1    localhost
172.16.1.1  myserver.myorg.org   myserver   srv
```

Файл hosts існує в ОС й сьогодні. В Unix-сумісних системах він розташований в каталозі /etc, в Windows-системах зазвичай розташований в каталозі %SystemRoot%\System32\drivers\etc.

У міру зростання Internet файли hosts також росли і створення масштабованого рішення для розпізнавання імен стало необхідністю. Таким

рішенням стала спеціальна служба – *система доменних імен* (Domain Name System, DNS).

DNS – централізована служба, заснована на розподіленої базі відображень “доменне ім'я” – “IP-адреса”.

Служба DNS використовує в своїй роботі протокол “клієнт – сервер”. У ньому визначені DNS-сервери та DNS-клієнти. DNS-сервери використовують розподілену базу відображень, а DNS-клієнти звертаються до серверів із запитами про дозвіл доменного імені в IP-адресу.

Служба DNS спирається на ієрархію доменів і кожен сервер служби DNS зберігає тільки частину імен мережі, а не всі імена, як це відбувалося при використанні файлів hosts.

Для кожного домену імен створюється свій DNS-сервер, який окрім таблиці відображення імен містить посилання на інші DNS-сервера.

Існує дві основні схеми дозволу DNS-імен:

– нерекурсивна або ітеративна;

– непряма (рос.: косвенная) або рекурсивна.

У першій схемі роботу з пошуку IP-адреси координує DNS-клієнт.

1. DNS-клієнт звертається до кореневого DNS-серверу із зазначенням FQDN.

2. DNS-сервер відповідає, вказуючи адресу наступного DNS-серверу, який обслуговує домен верхнього рівня, заданий в старшій частині запитаного імені.

3. DNS-клієнт робить запит до наступного DNS-серверу, який відсилає його до DNS-сервера потрібного піддомену і т.д., поки не буде знайдений DNS-сервер, в якому зберігається відповідність запитаного імені IP-адресу. Цей сервер дає остаточну відповідь клієнту.

Оскільки перша схема завантажує клієнта досить складною роботою, то вона застосовується рідко.

Друга схема:

1. DNS-клієнт запитує локальний DNS-сервер, тобто той сервер, який обслуговує піддомен, до якого належить ім'я клієнта.

2. Якщо локальний DNS-сервер знає відповідь, то він відразу ж повертає його клієнту.

3. Якщо локальний DNS-сервер не знає відповідь, то він виконує ітеративні запити до кореневого серверу і т.д. точно так же, як це робив клієнт в першій схемі. Отримавши відповідь, він передає його клієнту, який весь цей час просто чекав його від свого локального DNS-серверу.

Практично всі DNS-клієнти використовують рекурсивну процедуру.

Для прискорення пошуку IP-адрес DNS-сервери широко використовують процедуру кешування (хешування, рос.: кеширования, хеширования) відповідей, які проходять через них. Щоб служба DNS могла оперативно

відпрацьовувати зміни, що відбуваються в мережі, відповіді кешуються на певний час – зазвичай від декількох годин до декількох днів.

Зазвичай користувачі використовують в якості IP-адрес DNS-серверів своїх зон ті, що їм надають місцеві провайдери, або адміністратори. Саме ці DNS-сервери повинні швидко надати за запитом FQDN потрібні IP-адреси. Але буває така ситуація, коли з якихось технічних причин локальні служби DNS недоступні, а фізичне з'єднання з Internet присутнє. Тоді користувачі можуть тимчасово скористатися вільними загальнодоступними DNS-серверами. Наприклад, одними з таких відкритих DNS-серверів є Google Public DNS, що працюють з грудня 2009 року та за словами компанії Google забезпечують ефективне кешування запитів та підвищений захист. IP-адреси таких серверів наступні:

– IPv4: 8.8.8.8, 8.8.4.4;

– IPv6: 2001:4860:4860::8888, 2001:4860:4860::8844.

Списки загальних DNS серверів доступні за адресою: https://public-dns.info/

Слід пам'ятати, що використання загальнодоступних або невідомих DNS-серверів з низьким захистом є дуже небезпечним! Якщо DNS-сервер був взламаний, то існує небезпека підміни IP-адресу якогось символьного імені на IP-адресу вузла злодіїв та шахраїв. Слід також періодично перевіряти наявність інформації в локальному файлі hosts! Зазвичай багато вірусних програм можуть внести до нього хибну інформацію та перенаправити таким чином роботу браузера на шахрайські ресурси Internet!

Примітка: в лекції не розглядані питання, щодо налаштування та адміністрування DNS-серверів. Зазвичай ці питання розглядаються в курсі "Адміністрування операційних систем та мереж".

Лекція 10. Протоколи локальних мереж

Стандарти IEEE 802

У 1980 році в інституті IEEE був організований комітет 802 зі стандартизації технологій LAN. Результатом роботи комітету IEEE 802 стало прийняття сімейства стандартів IEEE 802.x, що містять рекомендації з проектування нижніх рівнів локальних мереж. Ці стандарти базувалися на узагальненні популярних фірмових стандартів, зокрема *Ethernet* (компанії Xerox) та *Token Ring* (компанії IBM). Крім IEEE у роботі по стандартизації протоколів LAN беруть участь й інші організації. Наприклад, для мереж, що працюють на оптоволокні, інститутом ANSI розроблений стандарт FDDI, що забезпечує швидкість передачі даних 100 Мбіт/с. Це був перший протокол LAN, який в 10 разів перевищив швидкість технології Ethernet. Структура стандартів IEEE 802 представлена на рис. 10.1.

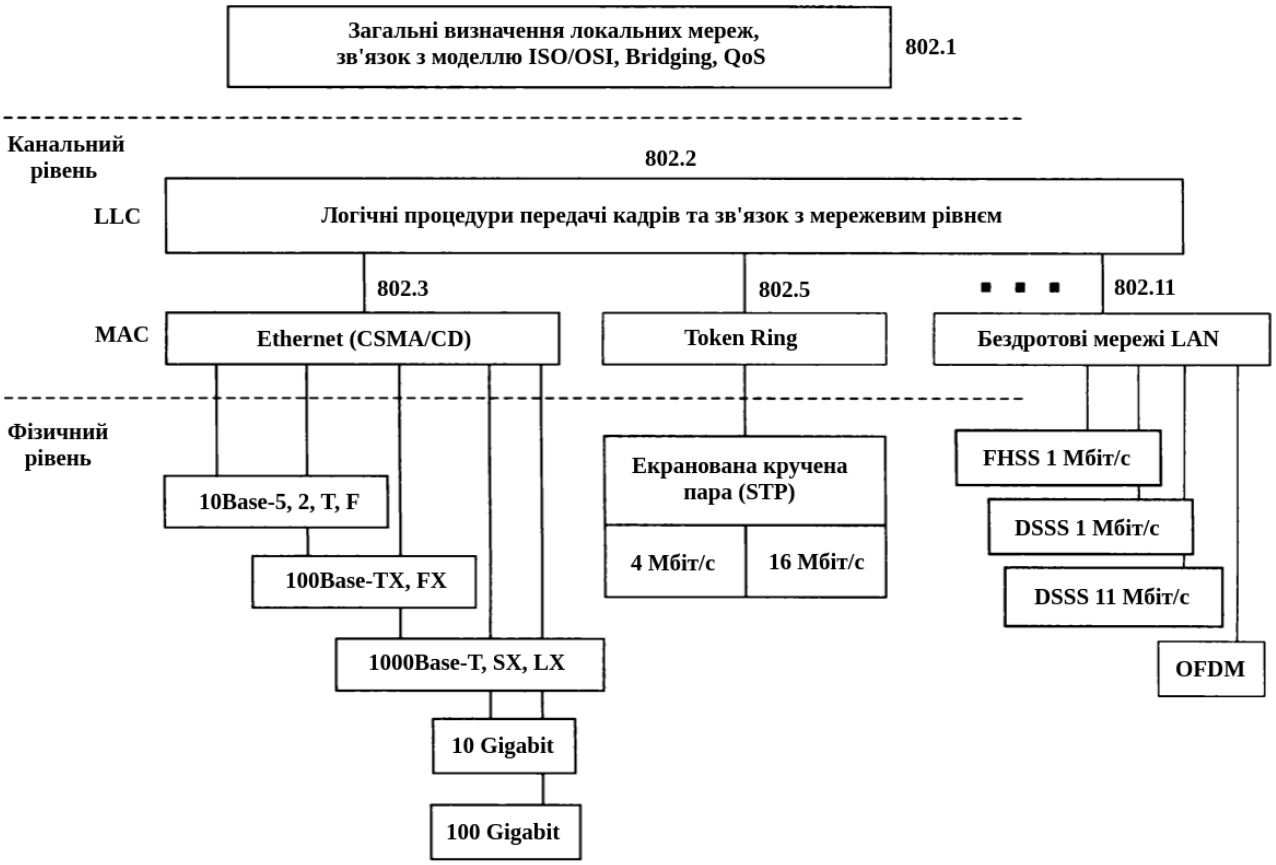

Рис. 10.1. Структура стандартів IEEE 802.x

Стандарт IEEE 802.1 є загальним документом, який визначає архітектуру та прикладні процеси системного управління мережею, методи об'єднання мереж на підрівні управління доступом передавального середовища. Відповідно до цього стандарту канальний рівень розбитий на два підрівні: УЛК (Управління логічним каналом) та УДС (Управління доступом до фізичного середовища).

Стандарт IEEE 802.2 визначає протокол управління логічним каналом, в тому числі специфікує інтерфейси на мережевому рівні та підрівні УДС.

Кожен з решти стандартів, починаючи з *IEEE 802.3* визначає метод доступу та специфіку фізичного рівня для конкретного типу LAN. Стандарт IEEE 802.3 описує характеристики та процедури МДКН/ОС (CSMA/CD).

IEEE 802.4 визначає протокол маркерного доступу до моноканалу.

IEEE 802.5 визначає протокол маркерного доступу до кільцевої мережі.

Для створення LAN, що охоплює площу радіусом до 25 км та використання технічного засобу кабельного ТБ існує стандарт *IEEE 802.6*.

IEEE 802.11 – стандарт на роботу бездротових локальних мереж (*WLAN*), визначення радіусу мережі для мобільних пристроїв.

IEEE 802.12 – стандарт на високошвидкісні комп'ютерні мережі 100VG- AnyLAN.

IEEE 802.15 – робоча група, що займається визначенням стандарту бездротових персональних мереж (WPAN), наприклад, розвиток технології Bluetooth. Та ін.

Стандарт IEEE 802.3

Ethernet найпоширеніший на сьогодні стандарт LAN. Цей мережевий стандарт, заснований на експериментальній мережі Ethernet Network, що розроблена компанією Xerox та реалізований в 1975 році. У 1980 фірми DEC, Intel та Xerox спільно розробили й опублікували стандарт Ethernet-2 (Ethernet Dix), на основі якого був розроблений стандарт IEEE 802.3. Залежно від типу фізичного середовища стандарт IEEE 802.3 має різні модифікації. Так, одного часу найбільш популярними специфікаціями фізичного середовища Ethernet для швидкості передачі даних 10 Мбіт/с, були наступні:

10Base-5 – "товстий" коаксіальний кабель діаметром 0,5 дюйма з хвильовим опором 50 Ом. Максимальна довжина сегмента: 500 м (без повторювачів). Максимальна кількість вузлів, що підключаються до сегменту – 100. Максимальна кількість сегментів – 5 (4 повторювачі), з яких тільки 3 можуть використовуватися для підключення вузлів, а 2-а грають роль подовжувачів мережі. Структура мережі на 10Base-5 представлена на рис. 10.2.

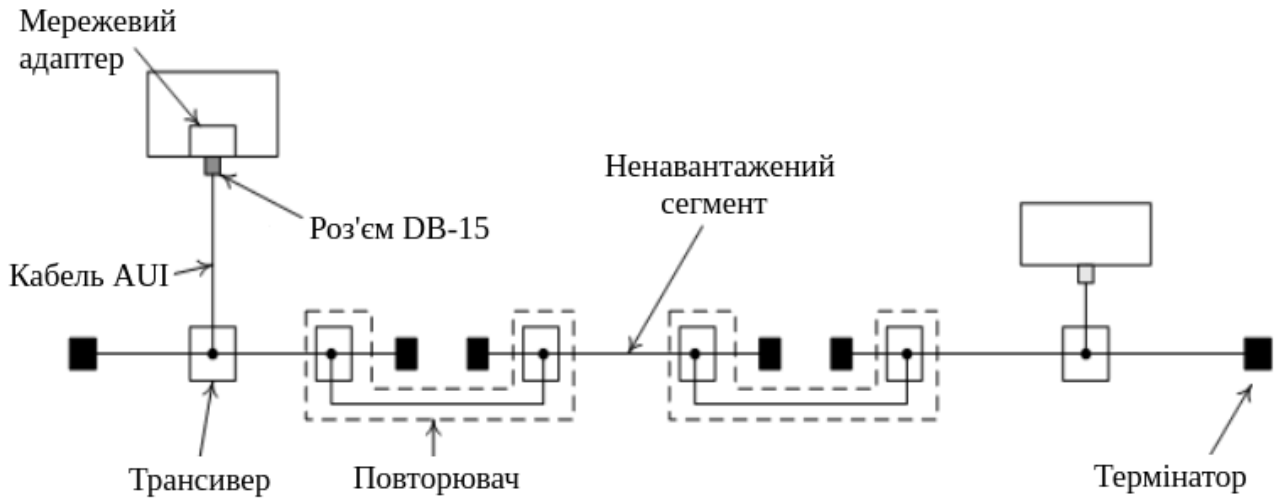

Рис. 10.2. Структура мережі за стандартом 10Base-5

10Base-2 – "тонкий" коаксіальний кабель діаметром 0,25 дюйма з хвильовим опором 50 Ом. Максимальна довжина сегмента: 185 м (без повторювачів). Максимальна кількість вузлів, що підключаються до сегменту – 30. Максимальна кількість сегментів – 5 (4 повторювачі), з яких тільки 3 можуть використовуватися для підключення вузлів, а 2-а грають роль подовжувачів мережі. Структура мережі на 10Base-2 представлена на рис. 10.3.

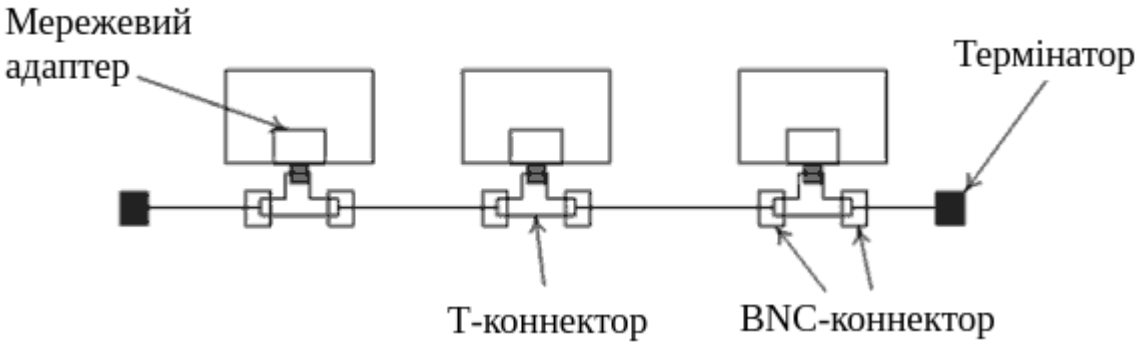

Рис. 10.3. Структура мережі за стандартом 10Base-2

10Base-T – кабель на основі неекранованої кручений пари (UTP). Утворює зіркоподібну топологію на основі концентратору (багатопортового повторювача). Відстань між концентратором та кінцевим вузлом – не більше 100 м. Між будь-якими двома вузлами мережі може бути не більше 4-х концентраторів (так зване "правило 4-х хабів"). Структура мережі на 10Base-T представлена на рис. 10.4, з використанням правила 4-х хабів – на рис. 10.5.

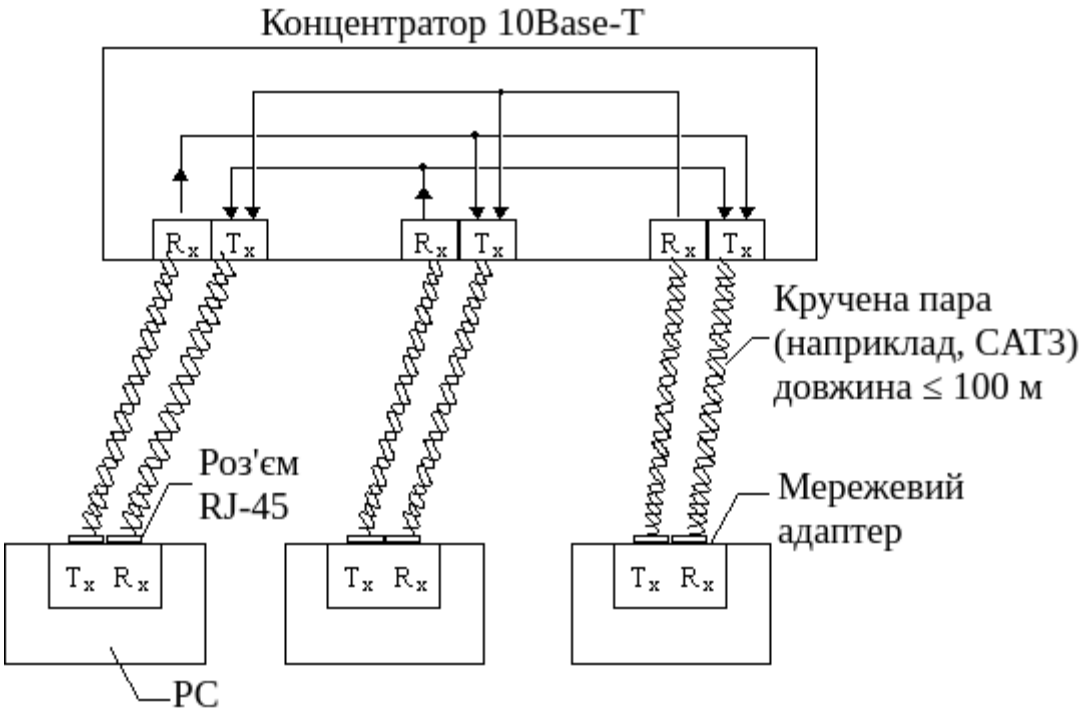

Рис. 10.4. Структура мережі за стандартом 10Base-T

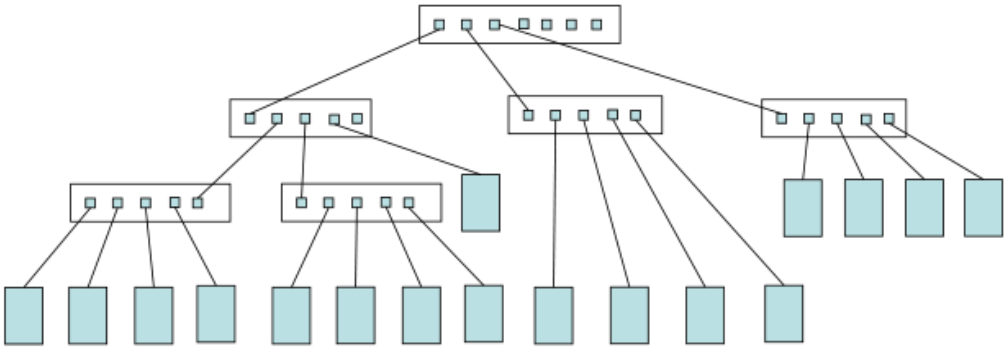

Рис. 10.5. Структура мережі 10Base-T з використанням декількох концентраторів (правило 4-х хабів)

10Base-F – волоконно-оптичний кабель. Топологія аналогічна топології стандарту 10Base-T, але відстань між концентратором та кінцевим вузлом може досягати 2 км. Правило 4-х хабів залишається в силі. Оптоволоконні стандарти в якості основного типу кабелю рекомендують досить дешеве багатомодове оптичне волокно, що володіє пропускною здатністю 500-800 МГц при довжині кабелю 1 км. Припустимо й більш дороге одномодове оптичне волокно з пропускною здатністю в кілька ГГц, але при цьому потрібно застосовувати спеціальний тип трансивера. Функціонально мережа Ethernet на оптичному кабелі складається з тих же елементів, що і мережа стандарту 10Base-T – мережевих адаптерів, багатопортового повторювача та відрізків кабелю, що з'єднують адаптер з портом повторювача. Як і у випадку крученої пари, для

з'єднання адаптера з повторювачем використовуються два оптоволокна – одне з'єднує вихід Tx адаптера зі входом Rx повторювача, а інше – вхід Rx адаптера з виходом Tx повторювача.

Стандарт *FOIRL* (Fiber Optic Inter-Repeater Link) являє собою перший стандарт комітету 802.3 для використання оптоволокна в мережах Ethernet. Він гарантує довжину оптоволоконного зв'язку між повторювачами до 1 км при загальній довжині мережі не більше 2500 м. Максимальна кількість повторювачів між будь-якими вузлами мережі – 4. Максимального діаметру в 2500 м можна досягти, хоча максимальні відрізки кабелю між усіма 4 повторювачами, а також між повторювачами та кінцевими вузлами неприпустимі – інакше вийде мережа довжиною 5000 м.

Стандарт *10Base-FL* представляє собою незначне поліпшення стандарту *FOIRL*. Збільшена потужність передавачів, тому максимальна відстань між вузлом та концентратором збільшилася до 2000 м. Максимальне число повторювачів між вузлами залишилося рівним 4, а максимальна довжина мережі – 2500 м.

Стандарт *10Base-FB* призначений тільки для з'єднання повторювачів. Кінцеві вузли не можуть використовувати цей стандарт для приєднання до портів концентратора. Між вузлами мережі можна встановити до 5 повторювачів 10Base-FB при максимальній довжині одного сегмента 2000 м та максимальній довжині мережі 2740 м.

Як і в стандарті l0Base-T, оптоволоконні стандарти Ethernet дозволяють з'єднувати концентратори тільки в деревоподібні ієрархічні структури. Будь-які петлі між портами концентраторів не допускаються.

Різновиди стандарту IEEE 802.11

Базовий стандарт 802.11 прийнятий в 1997 році і орієнтований на кілька бездротових середовищ (фізичний рівень – радіоканал): два види радіопередачі (FHSS – частотне розширення спектру та DSSS – розширення спектру з прямою послідовністю) відрізняються способом модуляції, але використовують однакову технологію розширення спектру, а також мережі з використанням інфрачервоного випромінювання.

Промислова група основних виробників обладнання для бездротових мереж на базі стандарту IEEE 802.11 відома в світі, як *Wi-Fi Alliance*.

Wi-Fi – Wireless Fidelity – "бездротова якість" або "бездротова точність" є торговою маркою цього альянсу.

IEEE 802.11 є набором стандартів зв'язку для комунікації через бездротову локальну мережеву зону частотних діапазонів 0.9, 2.4, 3.6 та 5 ГГц. Основні стандарти цього набору, прийняті після 1997 року, представлені в наступній таблиці.

Таблиця 10.1

Деякі найпопулярніші різновиди стандарту IEEE 802.11

*Стандарт IEEE**	*Робочий діапазон частот, ГГц*	*Макс. швидкість передачі, Мбіт/с*	*Примітка*
802.11a	5	до 54	Висока споживана потужність радіопередавачів для частот 5 ГГц, невеликий радіус дії
802.11b	2,4	до 11	Передбачає автоматичне зниження швидкості при погіршенні якості сигналу
802.11g	2,4	до 54	
802.11n	2,4-2,5 або 5	до 150 на одній антені, до 450 на 3-х антенах, до 600 на 4-х антенах	Можливість роботи в декількох режимах
802.11ac	5-6	до 450 на одній антені, до 1300 на 3-х антенах, до 6770 на 8-ми антенах	Гігабітний Wi-Fi
802.11ad	57 – 71	до 7000	Після перегляду діапазон 60 ГГц охоплює частоту від 57 до 71 ГГц. Діапазон частот підрозділяється на 6 (раніше 4) різних каналів в IEEE 802.11ad, кожен з них займає простір 2160 МГц і забезпечує пропускну здатність 1760 МГц.
802.11ax (Wi-Fi 6, Wi-Fi 6E)	2,4 та 5 (або від 1 до 7)	до 10747	Хоча номінальна швидкість передачі даних тільки на 37% вище, ніж в попередньому стандарті IEEE 802.11ac, очікується, що WiFi 6 дозволить в 4 рази збільшити середню пропускну здатність за рахунок більш ефективного використання спектра і поліпшень для щільного розгортання.

*повний список можна переглянути за посиланням: https://en.wikipedia.org/wiki/IEEE_802.11

IEEE 802.11n – поширена версія стандарту 802.11 для мереж Wi-Fi, затверджена 11 вересня 2009 року. Стандарт підвищує швидкість передачі даних практично вчетверо в порівнянні з пристроями стандартів *802.11g* (максимальна швидкість яких дорівнює 54 Мбіт/с), за умови використання в режимі 802.11n з іншими пристроями 802.11n. Теоретично він здатний забезпечити швидкість передачі даних до 600 Мбіт/с, застосовуючи передачу даних відразу по

чотирьох антенах. За однією антени – до 150 Мбіт/с. Пристрої 802.11n працюють в діапазонах 2,4-2,5 або 5,0 ГГц. Крім того, пристрої 802.11n можуть працювати в трьох режимах:

– успадковане (Legacy), в якому забезпечується підтримка пристроїв 802.11b/g та 802.11a;

– змішаному (Mixed), в якому підтримуються пристрої 802.11b/g, 802.11a та 802.11n;

– “чистому” режимі – 802.11n.

Ключовий компонент стандарту 802.11n під назвою *MIMO* (Multiple Input, Multiple Output – багато входів, багато виходів) передбачає застосування просторового мультиплексування з метою одночасної передачі декількох інформаційних потоків по одному каналу, а також багатопроменеве відображення, яке забезпечує доставку кожного біта інформації відповідному одержувачу з невеликою ймовірністю впливу перешкод та втрат даних. Саме можливість одночасної передачі і прийому даних визначає високу пропускну здатність пристроїв 802.11n.

IEEE 802.11ac – поширений стандарт бездротових комп'ютерних мереж сімейства 802.11 для мереж Wi-Fi на частотах 5-6 ГГц, офіційно прийнятий 1 січня 2014 року. Пристрої, які працюють за цим стандартом, забезпечують швидкість передачі даних до 1.3 Гбіт/с (до 6 Гбіт/с 8х *MU-MIMO* – розраховані на багато користувачів системи з багатьма входами та багатьма виходами), що багаторазово вище, ніж в 802.11n. Стандарт передбачає використання до 8 антен MU-MIMO та розширення каналу до 80 і 160 МГц.

Виділяють три види організації бездротової локальної мережі (WLAN):

– епізодична мережа (Ad-Hoc або IBSS – Independent Basic Service Set);

– основна зона обслуговування Basic Service Set (BSS) або Infrastructure Mode;

– розширена зона обслуговування ESS – Extended Service Set.

Режим Ad-Hoc (IBSS або Peer-to-Peer – режим "рівний-з-рівним") – найпростіша структура локальної мережі, коли абонентські станції (ноутбуки, комп'ютери т.ін. пристрої) взаємодіють безпосередньо один з одним. Така структура зручна для термінового розгортання мереж. Для її створення необхідний мінімум обладнання – кожна абонентська станція повинна мати в своєму складі адаптер WLAN (рис. 10.6).

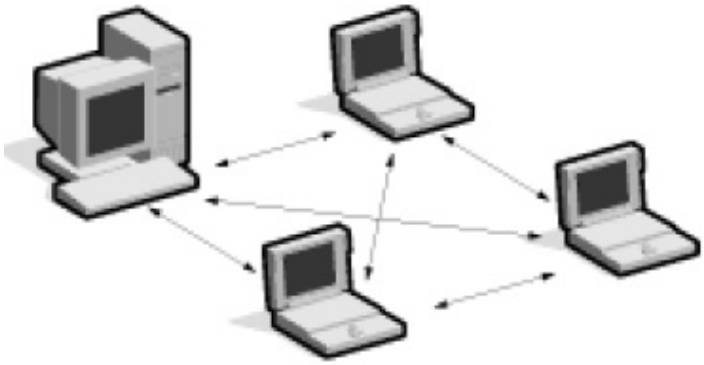

Рис. 10.6. Ad-Hoc (IBSS)

У режимі BSS вузли мережі взаємодіють один з одним не безпосередньо, а через точку доступу – AP (Access Point) – так звана Hot-spot організація. Точка доступу передає ідентифікатор мережі SSID (Service Set ID) за допомогою спеціальних сигнальних пакетів. Бездротові пристрої підключаються до AP, використовуючи її ідентифікатор мережі SSID, і обмінюються інформацією один з одним. В цьому випадку AP використовується в якості центральної точки підключення бездротових пристроїв. У режимі BSS, AP може грати роль моста для підключення до зовнішньої кабельної мережі (рис. 10.7).

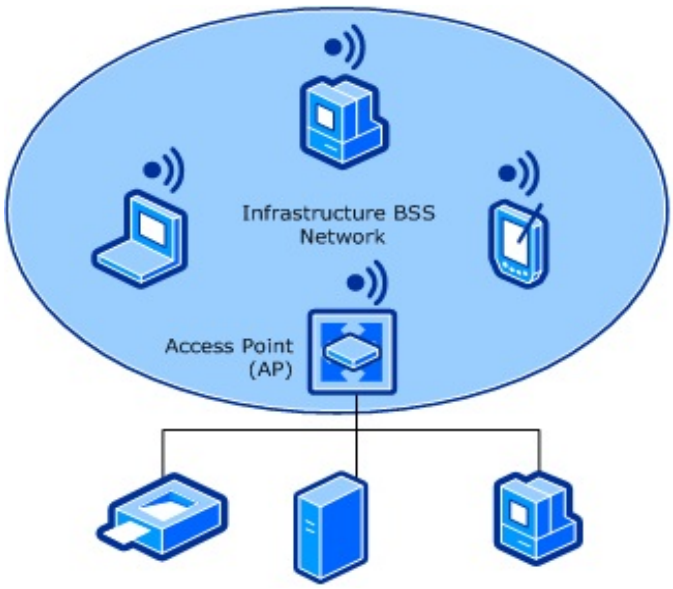

Рис. 10.7. Hot-Spot (BSS)

Режим ESS дозволяє об'єднати кілька точок доступу, тобто об'єднує кілька мереж BSS. В даному випадку точки доступу можуть взаємодіяти і один з одним. Розширений режим зручно застосовувати тоді, коли необхідно об'єднати в одну мережу кілька користувачів або підключити кілька провідних чи бездротових мереж (рис. 10.8).

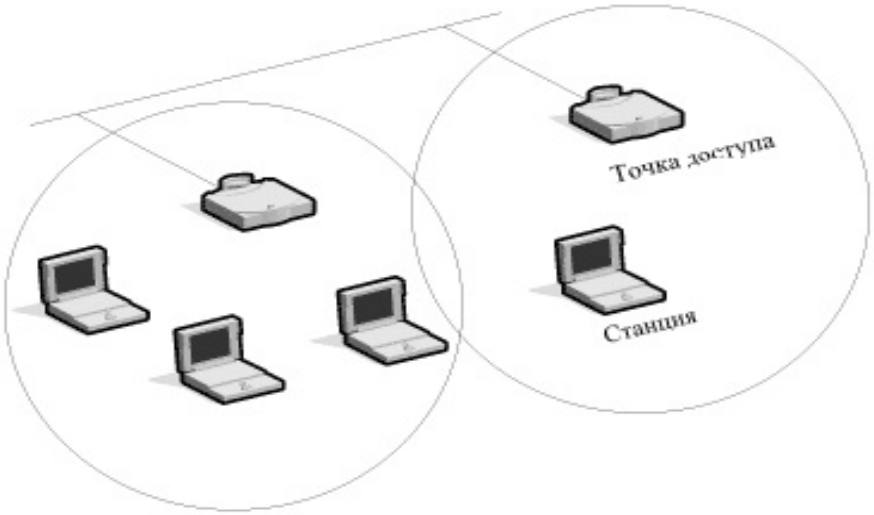

Рис. 10.8. ESS

Одним з основних питань при організації WLAN є розмір покриття. На цей параметр впливає відразу кілька факторів:

– частота використання (чим вона більша, тим менше дальність дії радіохвиль);

– наявність перешкод між вузлами мережі (різні матеріали по-різному поглинають та відображають сигнали);

– режим функціонування – Infrastructure Mode або Ad-Hoc;

– потужність передавального обладнання та чутливість приймаючого обладнання.

Наприклад, при ідеальних умовах поширення радіохвиль зона покриття однієї AP буде мати наступні значення:

– мережа стандарту IEEE 802.11a – 50 м,

– мережі 802.11b/g/n – близько 100 м.

Збільшуючи кількість точок доступу в режимі ESS або застосовуючи репіттери, можна розширювати зони покриття мережі на всю необхідну область охоплення.

Без підключення додаткової антени стійкий зв'язок для обладнання, наприклад, IEEE 802.11b, досягається в середньому на наступних відстанях.

1. Відкритий простір – 500 м.

2. Кімната, розділена перегородками з неметалічного матеріалу – 100 м.

3. Офіс з декількох кімнат – 30 м.

Слід мати на увазі, що через стіни з великим вмістом металевої арматури (в залізобетонних будівлях такими є несучі стіни) радіохвилі діапазону 2,4 ГГц іноді можуть взагалі не проходити, тому в кімнатах, розділених подібної стіною, доведеться ставити свої точки доступу або репіттери.

Для з'єднання віддалених LAN (або віддалених сегментів LAN) використовується обладнання зі спрямованими антенами, що дозволяє збільшити дальність зв'язку до 20 км (а при використанні спеціальних підсилювачів і великій висоті розміщення антен – до 50 км).

Комплекси для об'єднання LAN по топології діляться на "точку-точку" та "зірку". При топології "точка-точка" організовується радіоміст між двома віддаленими сегментами мережі. При топології "зірка" одна з РС є центральною і взаємодіє з іншими віддаленими РС. При цьому центральна РС має всеспрямовану антену, а інші віддалені РС – односпрямовані антени. Застосування всенаправленної антени у центральній станції обмежує дальність зв'язку дистанцією приблизно 7 км. Тому, якщо потрібно з'єднати між собою сегменти LAN, віддалені один від одного на відстань більше 7 км, доводиться з'єднувати їх за принципом "точка-точка". При цьому організовується бездротова мережа з кільцевою або іншою, більш складною, топологією.

У Wi-Fi передбачені як аутентифікація, так і шифрування. Шифрування значно знижує швидкість передачі даних, і, найчастіше, воно усвідомлено відключається адміністратором для оптимізації трафіку (але це погана практика).

Початковий стандарт шифрування WEP (Wired Equivalent Privacy) був дискредитований за рахунок вразливостей в алгоритмі розподілу ключів RC4. Це кілька пригальмувало розвиток Wi-Fi ринку і викликало створення інститутом IEEE робочої групи *802.11i* для розробки нового стандарту, що враховує уразливості WEP, що забезпечує 128-бітове AES шифрування та аутентифікацію для захисту даних. Wi-Fi альянс в 2003 представив свій власний проміжний варіант цього стандарту – WPA (Wi-Fi Protected Access). WPA

використовує протокол цілісності тимчасових ключів TKIP (Temporal Key Integrity Protocol). Також в ньому використовується метод контрольної суми MIC (Message Integrity Code), яка дозволяє перевіряти цілісність пакетів.

У 2004 Wi-Fi альянс випустив стандарт WPA2, який являє собою поліпшений WPA. Основна відмінність між WPA та WPA2 полягає в технології шифрування: TKIP і AES. WPA2 забезпечує більш високий рівень захисту мережі, так як TKIP дозволяє створювати ключі довжиною до 128 біт, а AES – до 256 біт.

В Україні використання Wi-Fi без дозволу Українського державного центру радіочастот можливо лише в разі використання АР зі стандартною всенаправленною антеною (<6 дБ, потужність сигналу ≤ 100 мВт на 2,4 ГГц та ≤ 200 мВт на 5 ГГц) для внутрішніх (використання всередині приміщення) потреб організації (Рішення Національної комісії з регулювання зв'язку України № 914 від 06.09.2007). У разі використання зовнішньої антени необхідно реєструвати передавач та отримати дозвіл на експлуатацію радіоелектронного засобу. Зауважмо, що законодавство може бути змінено, тому актуальну інформацію дивитися тут: https://www.ucrf.gov.ua/ua

Лекція 11. Технологія NAT (Network Address Translation)

Як було показано в лекції 7 на рис. 7.1, пакет IP має заголовок, що містить різноманітну інформацію, і в тому числі наступну:

– вихідну адресу – IP адресу мережевого інтерфейсу, наприклад, комп'ютера-джерела (нехай це буде 10.0.0.100);

– вихідний порт – номер TCP або UDP порту, призначений мережевим інтерфейсом, наприклад, комп'ютером-джерелом для цього пакету (нехай це буду порт 1080);

– адресу призначення – IP адресу мережевого інтерфейсу, наприклад, комп'ютера-приймача (нехай це буде 111.222.0.2);

– порт призначення – номер TCP або UDP порту, який просить відкрити мережевий інтерфейс, наприклад, комп'ютер-джерело на приймачі (нехай це буде порт 3021).

IP адреси визначають дві машини з кожного боку, в той час як номери портів гарантують, що з'єднання між цими двома комп'ютерами має унікальний ідентифікатор. Комбінація цих чотирьох чисел визначає єдине з'єднання TCP/IP. Кожен номер порту використовує 16 бітів, що означає, що існує 65536 (2^{16}) можливих значень. Насправді, так як різні виробники відображають порти трохи різними способами, можна очікувати близько 4000 доступних портів.

NAT (Network Address Translation; Трансляція Мережевих Адрес) – технологія Cisco, що використовується пристроєм (фаєрволом, маршрутизатором або комп'ютером), що знаходяться між внутрішньою мережею та іншою частиною світу для перетворення IP-адрес транзитних пакетів. Також в цьому контексті можна зустріти термін маскарадінг (IP Masquerading, Network Masquerading). Можна також знайти відмінності цих термінів. А саме:

Маскарад – заміна адреси на адресу машини, яка виконує маскарад.

Трансляція адрес – заміна адреси на будь-яку вказану.

Використовуючи термінологію Cisco, в контексті NAT є чотири основних визначення для IP-адрес. Розглянемо їх на прикладі, показаному на малюнку нижче. На обох маршрутизаторах робиться NAT.

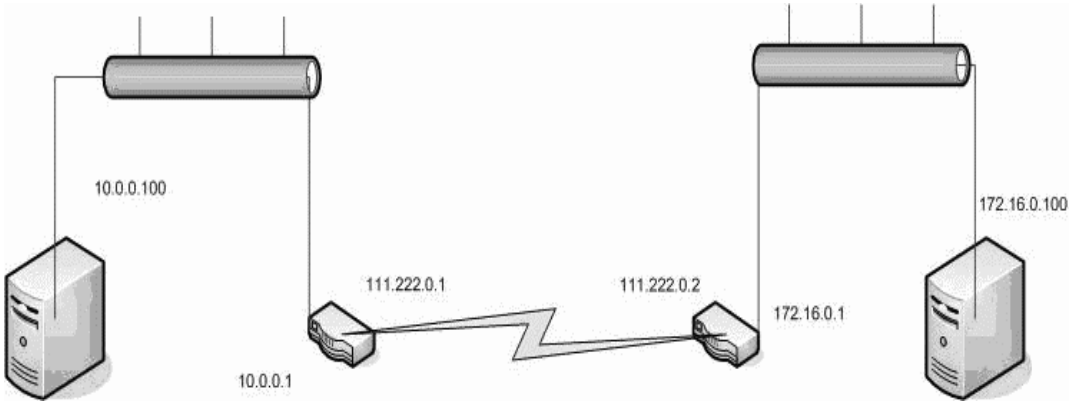

Рис. 11.1. Об’єднання двох локальних мереж через маршрутизатори

Розглянемо в контексті цієї технології, наступні основні терміни:

Inside Local (IL) – це адреса, яка присвоєна хосту, що знаходиться в локальній мережі (наприклад, адреси 10.0.0.100 та 172.16.0.100 – це адреси IL, рис. 11.1).

Inside Global (IG) – це зовнішня адреса, при відправленні пакетів на яку вони будуть доставлені, на хост з адресою IL (в прикладі для хосту 10.0.0.100 адресою IG є 111.222.0.1).

Outside Global (OG) – зовнішня адреса хосту, доступ до якого необхідно отримати з локальної мережі (в даному випадку, якщо відправляється пакет від 10.0.0.100 для 172.16.0.100, то адресою OG буде 111.222.0.2).

Outside Local (OL) – це адреса, під якою адреси зовнішніх хостів видно всередині локальної мережі (наприклад, якщо відправляють пакет від 10.0.0.100 для 172.16.0.100, то для хосту 172.16.0.100 це буде виглядати так, як ніби пакет прийшов від 172.16 .0.1 – з адреси OL).

Найпростіший випадок NAT – це трансляція адрес IL в IG і навпаки. При цьому маршрутизатор, виконує NAT, модифікує поле адреси в заголовку IP наступним чином:

1. У вихідних пакетах адреса джерела IL замінюється на IG, і пакет відправляється далі по роутингу до хосту з адресою OG.

2. У вхідних пакетах адреса приймача IG замінюється на IL і відправляється в локальну мережу для хосту з адресою IL.

Таким чином, в таблиці зіставлень NAT кожен запис складається з двох значень – IL та IG.

Описана або подібна схема іноді застосовується для забезпечення доступу зовні до хостів, що знаходяться в локальній мережі (наприклад, до веб-серверу або FTP-серверу). Вона може також застосовуватися для балансування навантаження шляхом динамічного розподілу пакетів, що приходять на публічну адресу маршрутизатора, між декількома серверами, що знаходяться в локальній мережі, і ще в деяких випадках.

Більш поширеним випадком є *NPAT (Network and Port Address Translation)*. При використанні NPAT в таблиці зіставлень кожен запис має не два (як в простому NAT), а п'ять значень:

1. Транспортний протокол.
2. Локальну адресу (IL).
3. Локальний порт.
4. Глобальну адресу (IG).
5. Глобальний порт.

Це дозволяє використовувати єдину публічну адресу для надання доступу в Internet з комп'ютерів, які знаходяться у локальній мережі. У документації Cisco така схема зазвичай називається "NAT with port overload" або коротше – "NAT overload". У більшості випадків мають на увазі саме його, коли вживають термін "NAT".

Варіанти реалізацій NAT

На прикордонному маршрутизаторі, що реалізує NAT, виділяють наступні чотири реалізації.

1. *Symmetric NAT* – в таблиці NAT маппінг адреси IL на адресу IG жорстко прив'язаний до адреси OG, тобто до адреси призначення, яка була вказана в вихідному пакеті, який ініціював цей маппінг.

Примітка: вважається, що це найбільш параноїдальна реалізація NAT, яка забезпечує більш високу безпеку для хостів локальної мережі, але в деяких випадках сильно ускладнює життя системних адміністраторів та користувачів.

2. *Full Cone NAT* – повна протилежність попередньої. У цій реалізації NAT у вхідних пакетах перевіряється тільки транспортний протокол, адреса призначення і порт призначення, адреса та порт джерела значення не мають. Вхідні пакети від будь-якого зовнішнього хосту будуть оттрансльовані та перенаправлені до відповідного хосту в локальній мережі, якщо в таблиці NAT присутній відповідний запис. Номер порту джерела в цьому випадку не має значення. Наприклад, якщо якась програма, що запущена на комп'ютері в локальній мережі, ініціювала отримання пакетів UDP від зовнішнього хосту 1.2.3.4 (рис. 11.2) на локальний порт 4444, то пакети UDP для цієї програми зможуть надсилати також і хости з 1.2.3.5, 1.2.3.6, та взагалі всі до тих пір, поки запис в таблиці NAT не буде видалений.

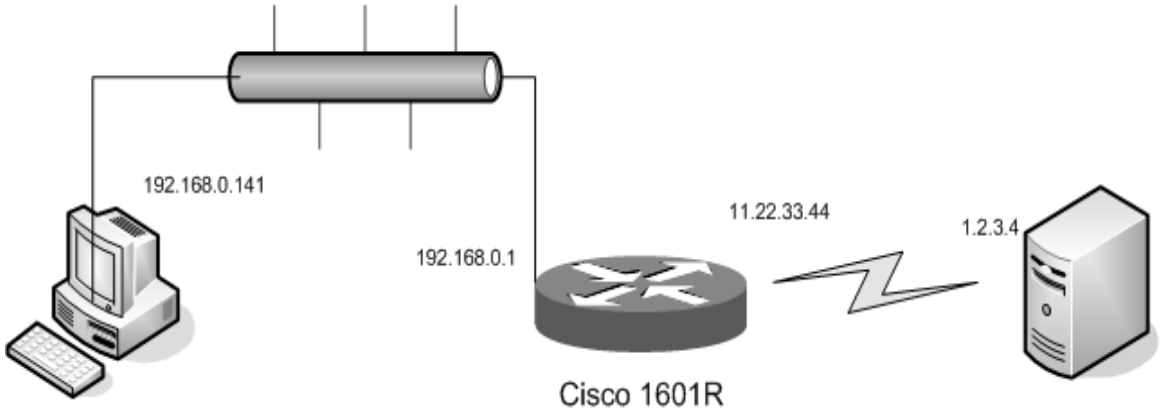

Рис. 11.2. Маршрутизатор Cisco з NAT

3. *Address Restricted Cone NAT (Restricted NAT)* – реалізація займає проміжне положення між Symmetric та Full Cone реалізаціями NAT – маршрутизатор буде транслювати вхідні пакети тільки з певної адреси джерела (наприклад, 1.2.3.4), але номер порту джерела при цьому може бути будь-яким.

4. *Port Restricted Cone NAT* (Port Restricted NAT) – те саме, що і Address Restricted Cone NAT, проте в цьому випадку маршрутизатор звертає увагу на відповідність номера порту джерела і не звертає уваги на адресу джерела.

Деяким програмам, які особливо призначені для IP-телефонії (оскільки там це найбільш актуально), важливо знати, чи знаходиться комп'ютер, на якому вони запущені, в локальній мережі за NAT або на комп'ютері з публічною IP адресою, та в разі NAT – визначити, якого він типу. Для цього можна використовувати протокол *STUN* (Simple Traversal of UDP through NAT – RFC 5389, RFC 3489), який дозволяє визначати наявність блокуючого firewall на прикордонному маршрутизаторі або на самому комп'ютері.

Фактично STUN – це клієнт-серверний протокол. VoIP-клієнт може включати в себе реалізацію клієнта STUN, який відправляє запит серверу STUN. Потім сервер STUN відправляє клієнту назад інформацію про те, яка зовнішня адреса маршрутизатору NAT та який порт відкритий на NAT для прийому вхідних запитів назад у внутрішню мережу.

TURN (Traversal Using Relay NAT) – це протокол, який дозволяє вузлу за NAT або брандмауером отримувати вхідні дані через TCP або UDP з'єднання. Така можливість особливо актуальна для вузлів позаду симетричних NAT, або брандмауерів, які збираються стати приймаючою стороною в з'єднанні з одним конкретним вузлом (peer-ом).

TURN не призначений для перекидання портів сервера через NAT, він підтримує з'єднання точка-точка між вузлами, які розташовані за NAT (як в IP-телефонії). У цьому плані він зберігає функції безпеки, забезпечені симетричним NAT та брандмауерами, але змінює таблиці трансляції так, щоб вузол на внутрішній стороні міг стати приймаючою стороною з'єднання.

Протокол TURN описаний в RFC 5766, оновлення TURN для підтримки IPv6 описано в RFC 6156. Схема URI для TURN документована в RFC 7065.

У деяких реалізаціях NAT існує спеціальна функція – трансляція адрес на рівні програм, яка також має назву NAT ALG (Application Level Gateways). При задіяній функції ALG, маршрутизатор відслідковує та модифікує дані рівня програм деяких мережевих протоколів. Ця функція в маршрутизаторах Cisco дозволяє здійснювати трансляцію адрес рівня програм, наприклад, для протоколу FTP, а також для протоколів SIP, H.323, Skinny та деяких інших (завдяки цьому можна, наприклад, розміщувати в локальній мережі сервери DNS). Для більшої зручності функція ALG, наприклад, в маршрутизаторах Cisco, включена за замовчуванням. Аналогічну ALG функціональність в маршрутизаторах на основі ОС Linux забезпечують додаткові модулі та патчі до ядер (наприклад, такі, як ip_masq_ftp, ip_masq_irc і т.п.).

NAT може працювати кількома способами:

1. Статичний NAT – відображення незареєстрованої IP адреси на зареєстровану IP адресу на підставі один до одного. Особливо корисно, коли пристрій повинен бути доступним зовні мережі. Наприклад, в статичному NAT, комп'ютер з адресою 192.168.32.10 буде завжди транслюватися в деяку задану адресу, наприклад, в 213.18.123.110.
2. Динамічний NAT – відображає незареєстровану IP адресу на зареєстровану адресу від групи зареєстрованих IP адрес. Динамічний NAT також встановлює безпосереднє відображення між незареєстрованою та зареєстрованою адресою, але відображення може змінюватися в залежності від зареєстрованої адреси, доступної в пулі адрес, під час комунікації. Наприклад, в динамічному NAT, комп'ютер з адресою 192.168.32.10 транслюється в перший доступний адрес в заданому діапазоні, наприклад, від 213.18.123.100 до 213.18.123.150.
3. Перевантаження (NAT overload) – форма динамічного NAT, який відображає кілька незареєстрованих адрес в єдину зареєстровану IP адресу, скориставшись різними портами. Відомий також як *PAT* (Port Address Translation). При перевантаженні, кожен комп'ютер в приватній мережі транслюється в ту ж саму задану адресу (наприклад, 213.18.123.100), але з різним номером порту.
4. Перенаправлення портів (Port Forwarding) – коли IP адреси, які використовуються у внутрішній мережі, також використовуються в іншій мережі, маршрутизатор повинен тримати таблицю пошуку цих адрес так, щоб він міг перехопити і замінити їх зареєстрованими унікальними IP адресами. Важливо відзначити, що NAT маршрутизатор повинен транслювати "внутрішні" адреси в зареєстровані унікальні адреси, а також повинен транслювати "зовнішні" зареєстровані адреси в адреси, які є унікальними для приватної

мережі. Це може бути зроблено або через статичний NAT, або можна використовувати DNS і реалізувати динамічний NAT.

Реалізація динамічного NAT автоматично створює міжмережевий захист між внутрішньою мережею та зовнішніми мережами або Internet. Динамічний NAT дозволяє тільки підключення, які породжуються в локальній мережі. По суті, це означає, що комп'ютер із зовнішньої мережі не може з'єднатися з комп'ютером в локальній, якщо той не почав з'єднання.

Статичний NAT, також званий вхідним маппінгом (inbound mapping), дозволяє підключення, ініційовані зовнішніми пристроями до комп'ютерів в LAN при певних обставинах. Наприклад, можна відобразити внутрішню глобальну адресу на певну внутрішню локальну адресу, яка призначена для Web-серверу.

Деякі NAT маршрутизатори передбачають велику фільтрацію та ведення логів трафіку. Фільтрація дозволяє компаніям контролювати, які сайти в мережі відвідують співробітники, перешкоджаючи їм переглядати будь-який матеріал. Можна використовувати реєстрацію трафіку, щоб створити журнал, які сайти відвідуються і на підставі цього генерувати різні звіти.

Іноді NAT плутають з проксі-серверами, де є певні відмінності. NAT прозорий для комп'ютерів джерела та приймача. Ніхто з них не знає, що має справу з третім пристроєм.

Але проксі-сервер не прозорий. Вихідний комп'ютер знає, що робить запит на проксі. Комп'ютер адресата думає, що проксі-сервер – це вихідний комп'ютер і має справу безпосередньо з ним. Крім того, проксі-сервери зазвичай працюють на транспортному рівні моделі OSI або вище, в той час як NAT – це протокол мережевого рівня. Робота на більш високих рівнях робить проксі-сервери повільнішими ніж NAT у більшості випадків.

Реальна вигода NAT в мережевому адмініструванні очевидна. Наприклад, можна перемістити Web-сервер або сервер FTP до іншого комп'ютера, не хвилюючись про розірваних з'єднаннях. Просто змінивши вхідний маппінг на нову внутрішню локальну адресу в маршрутизаторі, щоб відобразити новий хост. Можна також робити зміни у внутрішній мережі так, як будь-яка зовнішня IP-адреса або належить маршрутизатору або пулу глобальних адрес.

Розширені приклади реалізацій NAT[3]

1. Symmetric NAT

Кожний пакет з певної внутрішньої IP-адреси:порту на певну зовнішню IP-адресу:порт матиме після трансляції унікальну зовнішню адресу:порт. Відповідно, пакет з одієї і тієїж внутрішньої адреси:порту, але посланий на інший зовнішній хост або порт після трансляції матиме іншу зовнішню

3 За матеріалами ресурсу http://aoz.com.ua/

адресу:порт. Зовнішні хости можуть послати зворотній пакет тільки на ті адреси:порти звідки вони отримали пакети (рис. 11.3).

На рис. 11.3 – 11.6 позначками s та d вказані відповідно source IP-адреса:порт та destination IP-адреса:порт.

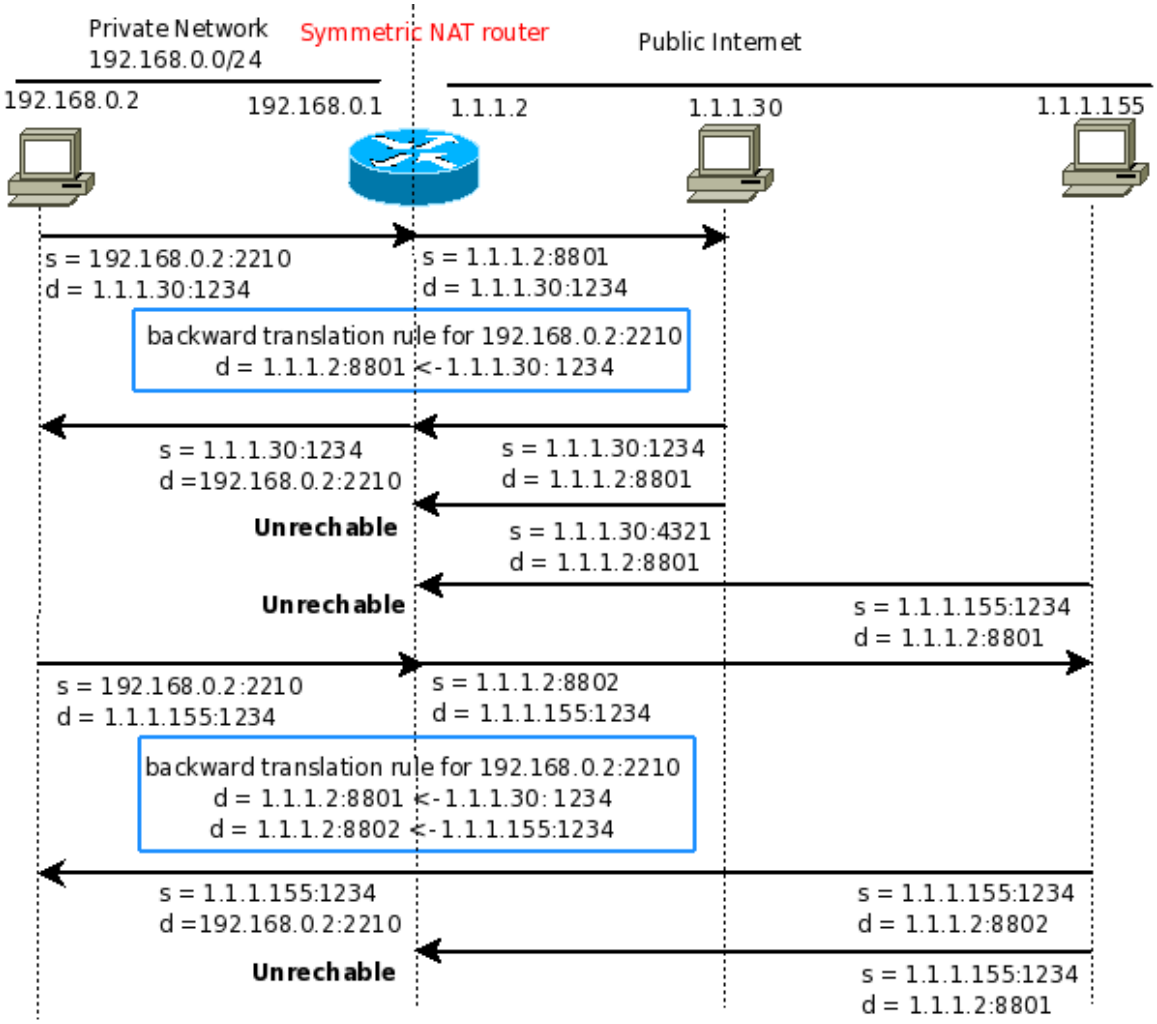

Рис. 11.3. Модель роботи Symmetric NAT

2. Full Cone NAT

Внутрішня адреса (192.168.0.2:2210) проектується на зовнішню адресу (1.1.1.2:8801). Будь-який пакет, який посланий з 192.168.0.2:2210 буде посланий через адресу 1.1.1.2:8801. Будь-який пакет з зовнішнього хосту, посланий на адресу 1.1.1.2:8801 буде відправлений на 192.168.0.2:2210 (рис. 11.4).

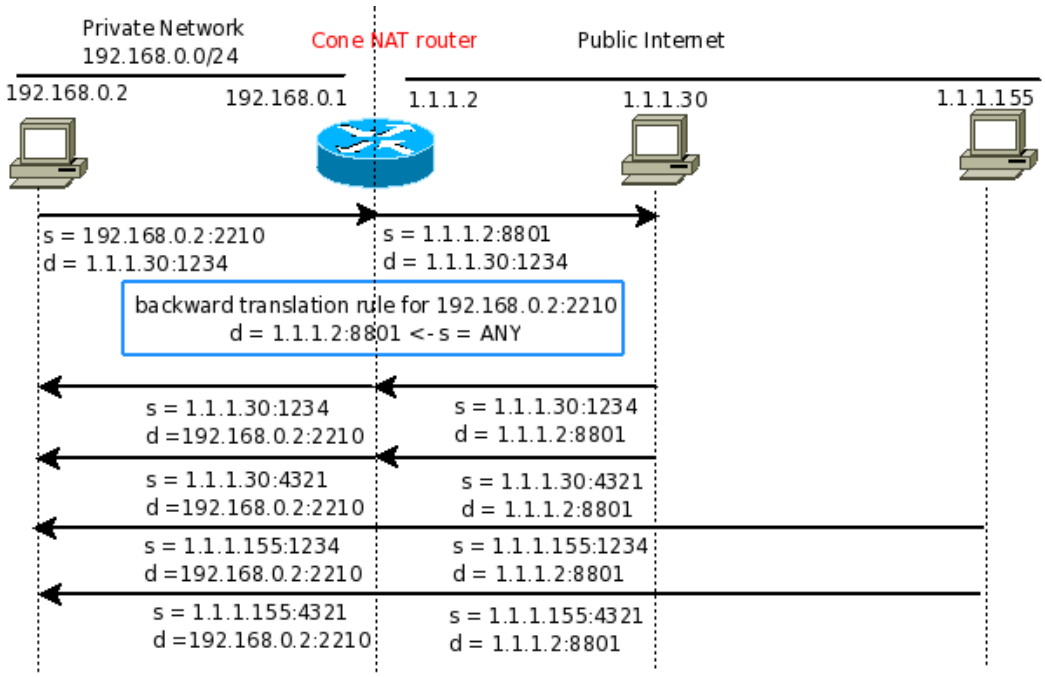

Рис. 11.4. Модель роботи Full Cone NAT

3. Address Restricted Cone NAT

Внутрішня адреса (192.168.0.2:2210) проектується на зовнішню адресу (1.1.1.2:8801). Будь-який пакет, що посланий з 192.168.0.2:2210 буде посланий через 1.1.1.2:8801. Пакет з будь-якого порту зовнішнього хосту, посланий на адресу 1.1.1.2:8801 буде відправлений на 192.168.0.2:2210 тільки в тому разі, якщо 192.168.0.2:2210 попередньо посилав пакет на цей зовнішній хост (рис. 11.5).

4. Port Restricted Cone NAT

Внутрішня адреса (192.168.0.2:2210) проектується на зовнішню адресу (1.1.1.2:8801). Будь-який пакет посланий з 192.168.0.2:2210 буде посланий через 1.1.1.2:8801. Зовнішній хост (1.1.1.30:1234) може послати пакет на 192.168.0.2:2210 через 1.1.1.2:8801 тільки в тому разі, якщо раніше 192.168.0.2:2210 посилав пакет на 1.1.1.30:1234 (рис. 11.6).

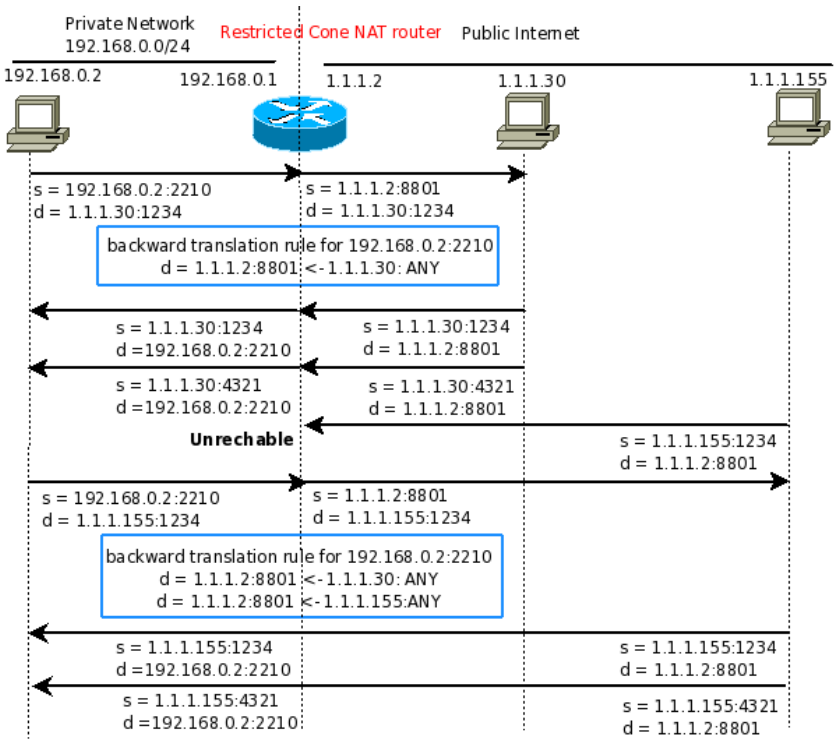

Рис. 11.5. Модель роботи Address Restricted Cone NAT

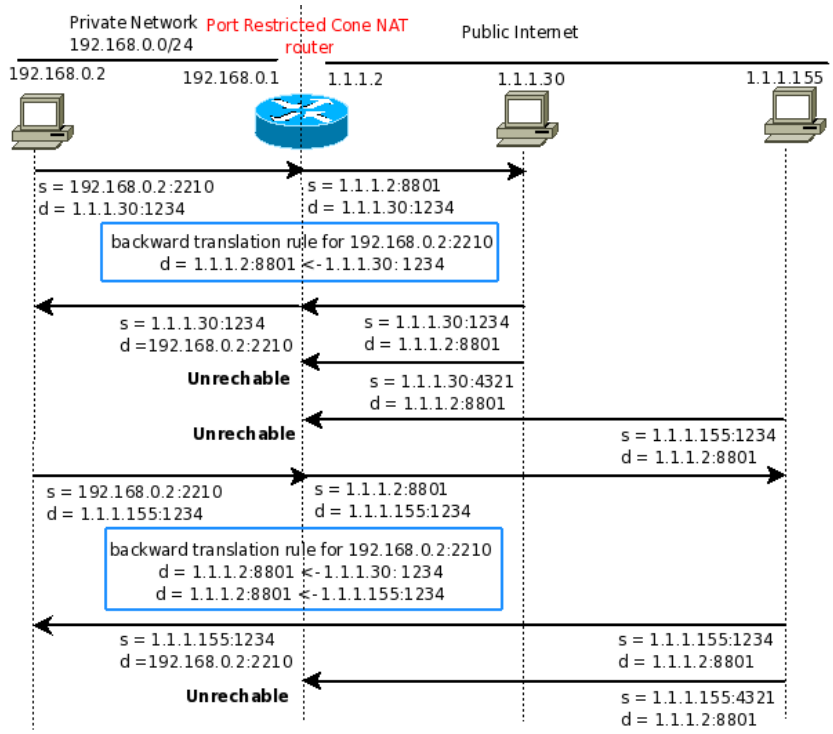

Рис. 11.6. Модель роботи Port Restricted Cone NAT

Як правило для керуванням NAT в маршрутизаторах призначена команда ip nat з різними параметрами. В Linux-подібних ОС NAT можна сконфігурувати за допомогою програм iptables, ufw, firewalld (firewall-cmd) та ін. У сучасних середовищах MS Windows для конфігурування NAT можна використовувати спеціальні команди PowerShell: New-NetNat, Add-NetNatStaticMapping, Get-NetNat та додаткові спеціальні програми.

Лекція 12. Проксі-сервери та брандмауери

Проксі-сервери

Проксі-сервер (від англ. Proxy – «представник, уповноважений») – служба в комп'ютерних мережах, що дозволяє клієнтам виконувати непрямі запити до інших мережних служб. Спочатку клієнт підключається до проксі-серверу та запитує який-небудь ресурс (наприклад, гіпертекстовий документ за http-посиланням), розташований на іншому сервері. Потім проксі-сервер або підключається до вказаного серверу та отримує ресурс у нього, або повертає ресурс із власного кешу (у випадках, якщо проксі має свій кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінений проксі-сервером в певних цілях. Також проксі-сервер дозволяє захищати клієнтський комп'ютер від деяких мережевих атак.

Найчастіше проксі-сервери застосовуються для наступних цілей:

1. Забезпечення доступу з комп'ютерів локальної мережі в Internet.
2. Кешування даних: якщо часто відбуваються звернення до одних та тих же зовнішніх ресурсів, то можна тримати їх копію на проксі-сервері і видавати за запитом, знижуючи тим самим навантаження на канал у зовнішню мережу та прискорюючи отримання клієнтом запитаної інформації.
3. Стиснення даних: проксі-сервер завантажує інформацію з Internet та передає інформацію кінцевому користувачеві в стислому вигляді. Такі проксі-сервери використовуються в основному з метою економії зовнішнього трафіку.
4. Захист локальної мережі від зовнішнього доступу: наприклад, можна налаштувати проксі-сервер так, що локальні комп'ютери будуть звертатися до зовнішніх ресурсів тільки через нього, а зовнішні комп'ютери не зможуть звертатися до локальних взагалі (вони «бачать» тільки проксі-сервер).
5. Обмеження доступу з локальної мережі до зовнішньої: наприклад, можна заборонити доступ до певних Web-сайтів, обмежити використання Internet якимось локальним користувачам, встановлювати квоти на трафік або смугу пропускання, фільтрувати рекламу та віруси.
6. Анонімізація доступу до різних ресурсів. Проксі-сервер може приховувати відомості про джерело запиту або користувача. В такому випадку цільової сервер бачить лише інформацію про проксі-сервер, наприклад, IP-адресу, але не має можливості визначити дійсне джерело запиту. Існують також варіанти проксі-серверів, які спотворюють інформацію – передають цільовому серверу неправдиву інформацію про справжніх користувачів.

Багато проксі-серверів використовуються для кількох цілей одночасно. Деякі проксі-сервери обмежують роботу декількома портами: 80 (HTTP), 443 (Шифроване з'єднання HTTPS), 20, 21 (FTP). На відміну від шлюзу, проксі-сервер найчастіше не пропускає ICMP-трафік (неможливо перевірити доступність машини, наприклад, командою ping).

Проксі-сервер, до якого може отримати доступ будь-який користувач мережі Internet, називається *відкритим*.

Прозорий проксі (transparent proxy) – це такий проксі-сервер, який приймає трафік від клієнтів мережі через маршрутизатор, здатний розрізняти який трафік повинен бути спрямований через проксі-сервер. Тобто клієнту не потрібно проводити конфігурацію ПЗ для роботи через проксі-сервер, маршрутизатор сам направить трафік клієнта на проксі-сервер (тобто для клієнта це прозорий проксі, але всеж потрібно налаштовувати окремо маршрутизатор).

Найбільш відомі та поширені проксі-сервери:

– Squid (open source) – функціонує практично на всіх сучасних ОС;

– 3proxy (open source);

– Kerio Control (пропрієтарний, включає проксі-сервер);

– WinGate (напівпропрієтарний, Windows platform, включає проксі-сервер);

– UserGate UTM (пропрієтарний, включає проксі-сервер);

– CCProxy (пропрієтарний, Windows platform);

– Microsoft Proxy Server, ISA Server, Microsoft Forefront Threat Management Gateway – застаріли продукти Microsoft (на момент 2020 вже неактуальні та не підтримуються).

Існують й окремі невеличкі open source Unix-подібні ОС, в яких також є функція проксі: pfSense, OPNsense, IPFire та ін.

Типи проксі

1. NAT proxy – найпростіший вид проксі. Входить до складу Windows починаючи з версії 2000. Називається «Загальний доступ до підключення інтернету» і включається опцією у властивостях з'єднання. Цей проксі працює прозоро для користувача, ніяких спеціальних налаштувань в програмах не потрібно.

2. HTTP proxy – найбільш поширений тип проксі (працює по протоколу HTTP). Якщо в програмі явно не прописаний тип використовуваного при роботі проксі, то це саме HTTP проксі.

3. HTTPS proxy (SSL proxy) – HTTP проксі з підтримкою шифрування по протоколу SSL.

4. IRC proxy (bouncer, bnc) – використовується для приховування реального IP в IRC мережах. Корисна властивість баунсерів – вони дозволяють залишатися на каналі навіть при виключенні IRC клієнта.

5. SOCKS proxy – можуть працювати з будь-якими протоколами (версія SOCKS4 – тільки TCP/IP, SOCKS5 – TCP/IP + UDP + авторизація + віддалений DNS-запит). До числа недоліків SOCKS proxy можна віднести складність їх використання. Використовуючи спеціальні програми можна соксіфіціровати

практично будь-яку програму. Такі проксі анонімні за визначенням, тому що не прив'язані до протоколів високого рівня і не модернізують заголовки запитів.
6. CGI proxy (анонімайзери) – з цим типом проксі можливо працювати тільки через браузер, оскільки в якості проксі сервера в даному випадку виступає не служба, що прослуховує певний порт, а скрипт на Web-сервері. Дуже прості у використанні, але мають істотно менші можливості, ніж всі інші види проксі, не завжди коректно відображають сторінки. Зате є можливість заборонити cookie та/або рекламу відразу в самому проксі сервері, не змінюючи налаштувань браузера.

Відмінності між типами proxy-серверів:

– CGI proxy – адреса такого проксі починається з http:// або https:// та містить шлях до web-сторінки (наприклад: http://www.server.com/nph-proxy.cgi). Анонімайзер (як правило) не має номера порту;

– HTTP та SOCKS proxy – їх адреси складаються з імені сервера та номера порту, які розділені між собою зазвичай двокрапкою (рідше – пропуском); наприклад: www.server.com:5731;

– SOCKS proxy – в 90% випадків мають номер порту 1080, 1081 або аналогічний;

– HTTP proxy – в 90% випадків мають номер порту 80, 8080, 81 або 3128;

Визначити тип proxy-сервера можна, скориставшись спеціальною програмою – proxy checker-ом.

Брандмауери

Firewall (брандмауер), міжмережевий екран або мережевий екран – це комплекс апаратних або програмних засобів, що захищає комп'ютер від несанкційованого доступу з зовнішньої мережі. Його мета – забезпечити безпеку: не пропустити в комп'ютер віруси, спам, хакерів і т.п.

Firewall може контролювати вхідний та вихідний трафік, вирізати рекламу. Таким чином, він здійснює контроль та фільтрування мережевих пакетів, які проходять через нього на різних рівнях моделі OSI відповідно до заданих правил. Деякі мережеві екрани також дозволяють здійснювати NAT і його різновиди.

Мережеві екрани підрозділяються на різні типи залежно від таких характеристик:

– забезпечує екран з'єднання між одним вузлом і мережею або між двома або більше різними мережами;

– відбувається контроль потоку даних на мережевому рівні або більш високих рівнях моделі OSI;

– чи аналізуються стани активних з’єднань чи ні.

Залежно від охоплення контрольованих потоків даних, мережеві екрани

поділяються на:

1. Традиційний мережевий (або міжмережевий) екран – програма (або невід'ємна частина ОС) на шлюзі (сервері, який передає трафік між мережами) або апаратне рішення, яка контролює вхідні та вихідні потоки даних між підключеними мережами.

2. Персональний мережевий екран – програма, встановлена на комп'ютері користувача і призначена для захисту від несанкціонованого доступу тільки цього комп'ютера.

Вироджений випадок – використання традиційного мережевого екрану сервером, для обмеження доступу до власних ресурсів.

Залежно від рівня, на якому відбувається контроль доступу, існує поділ на мережеві екрани, що працюють на:

– мережевому рівні, коли фільтрація відбувається на основі адрес відправника та одержувача пакетів, номерів портів транспортного рівня моделі OSI і статичних правил, заданих адміністратором;

– сеансовому рівні – відстежують сеанси між програмами, які не пропускають пакети, що порушують специфікації TCP/IP і часто використаних в зловмисних операціях – скануванні ресурсів, зломи через неправильні реалізації TCP/IP, обрив/уповільнення з'єднань, ін'єкція даних;

– рівні програм – фільтрація на підставі аналізу даних програми, що передаються всередині пакету. Такі типи екранів дозволяють блокувати передачу небажаної і потенційно небезпечної інформації, на підставі політик і налаштувань.

Деякі рішення, що відносяться до мережевих екранів рівня програми, представляють собою проксі-сервери з деякими можливостями мережного екрану, реалізуючи прозорі проксі-сервери, зі спеціалізацією по протоколам. Можливості проксі-сервера та багатопротокольна спеціалізація роблять фільтрацію значно більш гнучкою, ніж на класичних мережевих екранах, але такі програми мають всі недоліки проксі-серверів.

Залежно від відстеження активних з’єднань, мережеві екрани поділяють на:

– stateless (проста фільтрація) – не відслідковують поточні з'єднання (наприклад, TCP), а фільтрують потік даних виключно на основі статичних правил;

– stateful, stateful packet inspection (SPI) (фільтрація з урахуванням контексту) – з відстеженням поточних з'єднань і пропуском тільки таких пакетів, які задовольняють логіці та алгоритмам роботи відповідних протоколів й програм. Такі типи мережевих екранів дозволяють ефективніше боротися з різними видами DDoS -атак і вразливостями деяких мережевих протоколів. Крім того, вони забезпечують функціонування таких протоколів, як H.323, SIP, FTP та т.ін., які використовують складні схеми передачі даних між адресатами, що погано піддаються опису статичними правилами, і, найчастіше, несумісних зі стандартними stateless мережевими екранами.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Andrew S. Tanenbaum, David J. Wetherall. Computer Networks, 5th Edition. – Prentice Hall, Indian International Ed., 2010. – 960 p. ISBN-10: 9332518742, ISBN-13: 978-8131770221.

2. Ramon Nastase. Computer Networking: Beginner’s guide for Mastering Computer Networking and the OSI Model. – Independently published, 2018. – 219 p. ISBN-10: 1731076452, ISBN-13: 978-1731076458.

3. Ramon Nastase. Cisco CCNA Command Guide: An Introductory Guide for CCNA & Computer Networking Beginners. – Independently published, 2018. – 74 p. ISBN-10: 1731124279, ISBN-13: 978-1731124272.

4. Ramon Nastase. IP Subnetting for Beginners: Your Complete Guide to Master IP Subnetting in 4 Simple Steps. – Independently published, 2018. – 67 p. ISBN-10: 1791770088, ISBN-13: 978-1791770082.

5. Організація комп’ютерних мереж [Електронний ресурс]: підручник: для студ. спеціальності 121 «Інженерія програмного забезпечення»та 122 «Комп’ютерні науки» / КПІ ім. Ігоря Сікорського; Ю.А. Тарнавський, І.М. Кузьменко. – Електронні текстові дані (1 файл: 45,7 Мбайт). – Київ: КПІ ім. Ігоря Сікорського, 2018. – 259 с.

6. А.Г. Микитишин. Комп’ютерні мережі [навчальний посібник] / А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник. – Львів, «Магнолія 2006», 2013. – 256 с.

7. Jesin A. Packet Tracer Network Simulator. – Packt Publishing, 2014. – 134 p. ISBN-10: 1782170421, ISBN-13: 978-1782170426.

8. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 1. – Cisco Press, 2019. – 848 p. ISBN-10: 0135792738, ISBN-13: 978-0135792735.

9. Wendell Odom. CCNA 200-301 Official Cert Guide, Volume 2. – Cisco Press, 2019. – 624 p. ISBN-10: 1587147130, ISBN-13: 978-1587147135.

10. Гаркуша І.М. Методичні рекомендації і завдання до виконання лабораторних робіт з дисципліни "Комп’ютерні мережі" для студентів спеціальностей "Комп’ютерний еколого-економічний моніторинг" та "Інтелектуальні системи прийняття рішень" (напрям 6.050101 "Комп’ютерні науки"). – Д.: Національний гірничий університет, 2008. – 88 с.

11. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч.1. – 60 с.

12. Цвіркун Л.І. Комп’ютерні мережі. Методичні рекомендації до виконання лабораторних робіт студентами галузі знань 12 Інформаційні технології спеціальності 123 Комп’ютерна інженерія: у 2 ч. / Л.І. Цвіркун, Я.В. Панферова; М-во освіти і науки України, Нац. техн. ун-т «Дніпровська політехніка». – Дніпро: НТУ «ДП», 2018. – Ч.2. – 39 с.

Навчальне видання

Гаркуша Ігор Миколайович

Конспект лекцій
з дисципліни
“Комп’ютерні мережі”
для студентів галузі знань 12 “Інформаційні технології”
спеціальності 126 “Інформаційні системи та технології”

Електронний ресурс

Видано
у Національному технічному університеті
«Дніпровська політехніка».
Свідоцтво про внесення до Державного реєстру ДК №1842 від 11.06.2004.
49005, м. Дніпро, просп. Дмитра Яворницького, 19.