Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя

факультет прикладних інформаційних технологій та електроінженерії
(повна назва факультету)
кафедра автоматизації технологічних процесів і виробництв
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

магістр
(назва освітнього ступеня)

на тему: «Розробка і аналіз мережевої системи автоматизованого управління з використанням протоколів множинного доступу (комплексна тема).»

Виконав(ла): студент(ка) VI курсу, групи КАм–61
спеціальності 151 «Автоматизація та комп'ютерно–інтегровані технології»
(шифр і назва спеціальності)

		Немеришин А.В.
	(підпис)	(прізвище та ініціали)
		Замора О.Ю.
	(підпис)	(прізвище та ініціали)
Керівник		Дмитрів О.Р..
	(підпис)	(прізвище та ініціали)
Нормоконтроль		Козбур В.Р.
	(підпис)	(прізвище та ініціали)
Завідувач кафедри		Савків В.Б.
	(підпис)	(прізвище та ініціали)
Рецензент		Голотенко О.С..
	(підпис)	(прізвище та ініціали)

Тернопіль
2023

АНОТАЦІЯ

Множинний доступ припускає поділ ресурсів каналу між абонентами. Такий поділ каналів може бути частотним, часовим або кодовим. Множинний доступ застосовується й у провідних й у бездротових мережах. Розрізняють безконфліктні й конфліктні методи доступу. Безконфліктні методи множинного доступу використовують у стільникових мережах стандартів AMPS, NAMPS, GSM (у режимі передачі мови) і інших. Серед конфліктних методів доступу широке поширення отримав стандарт для локальних провідних мереж IEEE 802.3 (Ethernet) і стандарт для локальних бездротових мереж – IEEE 802.11 . У цей час іде активне впровадження стандарту для бездротових MAN–Мереж – IEEE 802.16 . Даний стандарт, як і стандарт для провідних мереж IEEE 802.14 , характеризується наявністю центральної станції. Особливістю стандартів IEEE 802.16 і IEEE 802.14 для мереж із центральною станцією (централізовані мережі) є використання конкурентного інтервалу в процесі передачі. У конкурентному інтервалі абоненти передають запити до центральної станції на надання канальних ресурсів. Абонент передає запит випадковим образом. Якщо передачі запитів від різних абонентів накладаються один на одного, то виникає конфлікт. У цьому випадку абоненти роблять повторну передачу відповідно до певних правил.

Метою роботи є розробка й аналіз алгоритмів керування передачею запитів у конкурентному інтервалі, що використовують випадковий множинний доступ і забезпечують оперативну доставку запитів на центральну станцію. Завданнями дослідження є:

1). Аналіз функціонування відомого алгоритму ВМД із чергою для централізованих мереж.

2). Розробка алгоритмів ВМД, що забезпечують меншу затримку при доставці запиту, чим раніше відомі алгоритми.

3). Аналіз запропонованих алгоритмів для різних видів вхідного потоку.

ABSTRACT

Multiple access implies the sharing of channel resources between subscribers. This division of channels can be frequency, time or code. Multiple access is used in both wired and wireless networks. There are non–conflict and conflict access methods. Conflict–free methods of multiple access are used in cellular networks of standards (in speech transmission mode) and others. Among the conflicting access methods, the standard for local wired networks and the standard for local wireless networks – . At this time, the standard for wireless MAN–Networks is being actively implemented – . This standard, like the standard for leading networks, is characterized by the presence of a central station. A feature of the standards for networks with a central station (centralized networks) is the use of a competitive interval in the transmission process. In the competitive interval, subscribers send requests to the central station for the provision of channel resources.

The subscriber transmits the request randomly. If transmissions of requests from different subscribers overlap each other, a conflict occurs. In this case, subscribers retransmit according to certain rules.

The purpose of the work is the development and analysis of algorithms for controlling the transmission of requests in a competitive interval, which use random multiple access and ensure prompt delivery of requests to the central station. The tasks of the research are:

1). Analysis of the functioning of the well–known VMD algorithm with a queue for centralized networks.

2). The development of VMD algorithms that ensure a lower delay in the delivery of a request, the earlier the algorithms are known.

3). Analysis of the proposed algorithms for different types of input flow.

ЗМІСТ

СПИСОК СКОРОЧЕНЬ

Англомовні скорочення

CRC	–	Cyclic Redundancy Code
CSMA	–	Carrier Sense Multiply Access
CSMA/CD	–	Carrier Sense Multiply Access with Collision Detection
DLC	–	Data Link Layer
DLE	–	Data Link Escape
ETX	–	End TeXt
FDDI	–	Fiber Distributed Data Interface
FDM	–	Frequency Division Multiplexing
LAN	–	Local Area Network
LLC	–	Logical Link Control
MAC	–	Media Access Control
STX	–	Start TeXt
TDM	–	Time Division Multiplexing
WAN	–	World Area Network

ВСТУП

Мережева система керування (networked control system NCS) — це система керування , в якій контури керування замкнуті через мережу зв’язку. Визначальною особливістю NCS є те, що сигнали керування та зворотного зв’язку обмінюються між компонентами системи у вигляді інформаційних пакетів через мережу.

Функціональність типової NCS визначається використанням чотирьох основних елементів:

1. Датчики для отримання інформації,
2. Контролери , щоб забезпечити рішення та команди,
3. Приводи , для виконання команд управління і
4. Комунікаційна мережа для обміну інформацією.

Найважливішою особливістю NCS є те, що він з’єднує кіберпростір із фізичним простором, що дозволяє виконувати кілька завдань на великій відстані. Крім того, NCS усуває непотрібну проводку, зменшуючи складність і загальну вартість проектування та впровадження систем керування. ЇЇ також можна легко модифікувати або модернізувати, додавши до неї датчики, виконавчі механізми та контролери з відносно низькою вартістю та без істотних змін у їхній структурі. Крім того, забезпечуючи ефективний обмін даними між своїми контролерами, NCS можуть легко об’єднувати глобальну інформацію для прийняття розумних рішень у великих фізичних просторах.

Їх потенційне застосування є численним і охоплює широкий спектр галузей, таких як дослідження космосу та землі, доступ у небезпечних середовищах, автоматизація виробництва, дистанційна діагностика та усунення несправностей, експериментальні установки, домашні роботи, літаки, автомобілі, моніторинг виробничих підприємств і телеоперації. У той час як потенційні застосування NCS численні, перевірених застосувань небагато, і

реальна можливість у сфері NCS полягає в розробці реальних програм, які реалізують потенціал області.

Типи мереж зв'язку:

- Польові шини , наприклад CAN, LON тощо.
- IP/ Ethernet
- Бездротові мережі, наприклад Bluetooth, Zigbee та Z–Wave . У зв’язку з цим часто використовується термін бездротова мережева система керування (wireless networked control system – WNCS).

Концепція iSpace. Поява та розвиток Інтернету в поєднанні з перевагами NCS привернули інтерес дослідників у всьому світі. Разом із перевагами також виникло кілька проблем, що породило багато важливих тем дослідження. Нові стратегії керування, кінематика приводів у системах, надійність і безпека зв’язку, розподіл смуги пропускання, розробка протоколів передачі даних, відповідне виявлення несправностей і стратегії відмовостійкого керування, збір інформації в режимі реального часу та ефективна обробка даних датчиків – це деякі з них. Відповідні теми, вивчені поглиблено.

Включення комунікаційної мережі в контур управління зі зворотним зв'язком робить аналіз і проектування комплексу NCS складнішим, оскільки це накладає додаткові часові затримки в контурах управління або створює можливість втрати пакетів. Залежно від програми, затримки можуть серйозно погіршити продуктивність системи.

Щоб пом'якшити ефект затримки часу, в лабораторії ADAC при Університеті штату Північна Кароліна запропонували методологію проміжного програмного забезпечення планувальника посилення (gain scheduler middleware – GSM) і застосували її в iSpace. В Джорджійському технологічному інституті використовували предиктор Сміта, фільтр Калмана та регулятор енергії для виконання телеоперацій через Інтернет.

Крім цього деякі розробники використовували генетичний алгоритм для розробки контролера, який використовується в NCS. Багато інших дослідників

надали рішення, використовуючи концепції з кількох областей управління, таких як надійне керування, оптимальне стохастичне керування , прогнозне керування моделлю, нечітка логіка тощо.

Найважливішим і найважливішим питанням, пов’язаним із проектуванням розподілених NCS із поступово зростаючою складністю, є відповідність вимогам до надійності та надійності системи, гарантуючи при цьому високу продуктивність системи в широкому робочому діапазоні. Це змушує мережеві методи виявлення несправностей і діагностики, які є важливими для моніторингу продуктивності системи, привертати все більше уваги.

Для мережевих систем важливим є забезпечення максимальної швидкості передачі даних, при мінімальних втратах пакетів даних. У випадку використання мережевих систем автоматизованого управління, які працюють в режимі реального часу, часто виникають колізії доступу до мережевого середовища передачі даних. При одночасній передачі пакетів даних в мережеве середовище виникає конфлікт, що приводить до втрати пакетів даних. Після з певною затримкою абоненти мережі проводять повторну передачу пакетів, що різко знижує ефективність і швидкодію мережі. Тому розробляються спеціальні алгоритми і мережеві протоколи для роботи з конкурентним мультидоступом до мережевого середовища (не важливо це оптичне, кабельне чи бездродотове з’єднання).

Підсумовуючи, розробка спеціальних алгоритмів, мережевих протоколів для роботи з конкурентним мультидоступом забезпечує:

- ефективний засіб передачі даних від точки використання до точки обробки, що часто знижує витрати на отримання даних, оскільки можна використовувати стандартні списки та каталоги в центральному комунальному підприємстві;

- покращений зв’язок «людина–машина», коли доступні відповідні термінальні засоби, такі як графічні дисплеї, таким чином скорочуючи час розробки;
- засіб скорочення вартості великих обчислень, дозволяючи їх виконувати на більших комп’ютерах, що зменшує витрати на одиницю експлуатації завдяки їх збільшеній потужності та зменшує або усуває потребу в «накладенні».

Узагальнюючи, системи конкурентного мультидоступу в мережевих системах автоматизованого управління виявилися дуже потужним інструментом. У той час як самі інструменти змінюватимуться з часом (прикладом є пристрої, здатні покращити зв’язок між людиною та машиною), основна філософія спільної мережевої системи залишиться, і це є ключем до їх використання.

1 АНАЛІТИЧНА ЧАСТИНА

1.1 Загальні відомості про цифрові та комп’ютерні мережі

Ідея комп'ютерних мереж запозичена із практики використання магістрально–модульних систем, які служать для передачі даних від різних джерел інформації в ЕОМ і назад у режимі реального часу. Такі системи стали активно розвиватися з початку 60–х років минулого століття. Найбільш характерним прикладом може служити система CAMAC, де для передачі даних від або до великої кількості об'єктів, використовувалася загальне апаратне транспортне середовище (шина, як правило, паралельна). Строго говорячи, локальна мережа ЕОМ є частковим випадком магістрально модульної системи. Іншим джерелом могли служити канали зв'язку ЕОМ з периферійними приладами (наприклад, дисковими запам'ятовувальними пристроями або вилученими терміналами; досить згадати канал SCSI, що був розроблений у тому числі й для цілей збору даних). Слід зазначити принципове розходження між такими системами й мережами. В останньому випадку дані передаються від ЕОМ до ЕОМ. Важливим фактором для розвитку мереж з'явилася розробка пакетного принципу передачі даних, що був створений ще до початку Другої світової війни. Прототипом сучасних мереж, можливо, з'явилися термінальні мережі великих обчислювальних центрів.

Першою мережею, де застосований пакетний принцип передачі даних, була ARPANET (1969; Advanced Research Project Agency NETwork). Ця мережа мала всього 4 вузли. Приблизно тоді ж стали розроблятися протоколи послідовної, синхронної (SDLC) і асинхронної ("старт/стоп") передачі даних, інтелектуальні термінали й канальні концентратори. У рамках цих робіт були розроблені пристрої й програми доступу до середовища з поділом за часом (TDM– Time Division Multiplexing). Така схема доступу використовується практично у всіх багатозадачних операційних системах. Все це створило передумови для розробки реальних мереж. Метою будівництва мереж є

ефективне використання ресурсів машин, поєднуваних мережею, і підвищення надійності системи в цілому. Через мережу передаються тексти, повідомлення, файли, зображення, завдання, команди, відео– або акустичні дані. Мережі уможливлюють:

- доступ до загальних ресурсів (швидкодіючий друк, диски великої ємності, backup–системи, інформаційні сховища, сервери й т.д.);
- децентралізацію обчислювального процесу, можливість створення розподілених обчислювальних систем (системи GRID), підвищення надійності систем за рахунок резервування;
- інформаційний обмін у видавництвах, інформаційних агентствах, пошукових системах, між звичайними людьми, розкиданими по усьому світі, у системах збору й обробки наукових, метео– і геофізичних даних і т.д.;
- розподілене керування;
- всесвітні й локальні системи міжособистісного спілкування (пошта, IC, SMS та ін.).

Мережі по своїй належності діляться на локальні (LAN – Local Area Network), міські (MAN – Metropolitan Area Network), регіональні (WAN – Wide Area Network) і всесвітні (Інтернет). У цей час існує величезна розмаїтість мереж в тому числі і ті, котрі використовуються для систем автоматизованого управління іконтролю. Але є в них і щось загальне: практично всі вони базуються на пакетному принципі передачі даних. Пакет являє собою послідовність нулів і одиниць. Нулю й одиниці (часто їх називають логічним нулем і логічною одиницею) ставиться у відповідність певний рівень амплітуди або знак перепаду. У цьому зв'язку у всіх мережах доводиться вирішувати проблему виділення початку й кінця пакетів. Як правило, для цієї мети використовуються унікальні послідовності біт або унікальні коди. При цьому виникає проблема, коли подібні сигнатури зустрічаються в тілі пакета, адже це може викликати збій – система помилково може прийняти таку послідовність за

сигнал переривання обробки пакета. Завдання вирішується з використанням ESC–Послідовностей або техніки біт–стаффінга. ESC–Послідовність являє собою рядок із двох або більше символів, перший з яких, як правило, має код 27 (десятковий; ESC). Рядок має такий формат, що не може зустрітися в межах пакета; якщо ж така послідовність все–таки зустрічається, включається алгоритм, що забезпечує її перетворення до унікального виду. Ця послідовність служить для підміни сигнатури початку або кінця пакета, якщо вона зустрінеться в його поле даних. Техніка біт–стафинга припускає додавання в певних ситуаціях нульового або одиничного біта або використання певних комбінацій сигналів на фізичному рівні.

При передачі даних потрібно забезпечувати синхронізацію й стабілізацію рівня реєстрації. Синхронізація між передавачем і приймачем необхідна насамперед тому, що не кожному біту в переданому коді відповідає зміну рівня сигналу. А це може приводити до того, що одна зі сторін передасть N біт, а інша при цьому буде вважати, що прийняла $N-1$ або $N+1$ біт. Синхронізація тактових частот передавача й приймача найчастіше здійснюється самою кодовою послідовністю, що транспортує дані, або незалежно, як, наприклад, це робиться в мережах SDH.

Тому що між передавачем і приймачем не завжди є гальванічний зв'язок, середній рівень сигналу може дрейфувати залежно від числа попередніх нулів або одиниць. Такий дрейф може приводити до помилок, тому що в суперпозиції із шумами або наведеннями може перевищити рівень дискримінації, що відокремлює стану логічного нуля й одиниці.

Практично всі мережі так чи інакше вирішують проблему націлення даних (як правило, це визначає алгоритм доступу до мережного середовища).
У мережах для формування віртуального каналу й транспортування даних використовуються схеми з комутацією каналів і з комутацією пакетів. У випадку комутації каналів спочатку здійснюється формування зв'язку між ініціатором і адресатом і тільки потім починається обмін даними (або розмова

при телефонному з'єднанні). Як параметр при встановленні з'єднання використовується код місця призначення, наприклад, його телефонний номер або IP–Адреса.

1.2 Модель ISO/OSI

OSI розшифровується як Open Systems Interconnection . Він був розроблений ISO – «Міжнародною організацією зі стандартизації» в 1984 році. Це 7–рівнева архітектура, кожен з яких має певну функціональність для виконання. Усі ці 7 рівнів працюють разом, щоб передавати дані від однієї людини до іншої по всьому світу.

Модель OSI, створена в 1984 році ISO, є еталонною структурою, яка пояснює процес передачі даних між комп'ютерами. Він розділений на сім рівнів, які працюють разом для виконання спеціалізованих мережевих функцій, що забезпечує більш систематичний підхід до роботи в мережі.

Рисунок 1.1 – Еталонна модель OSI

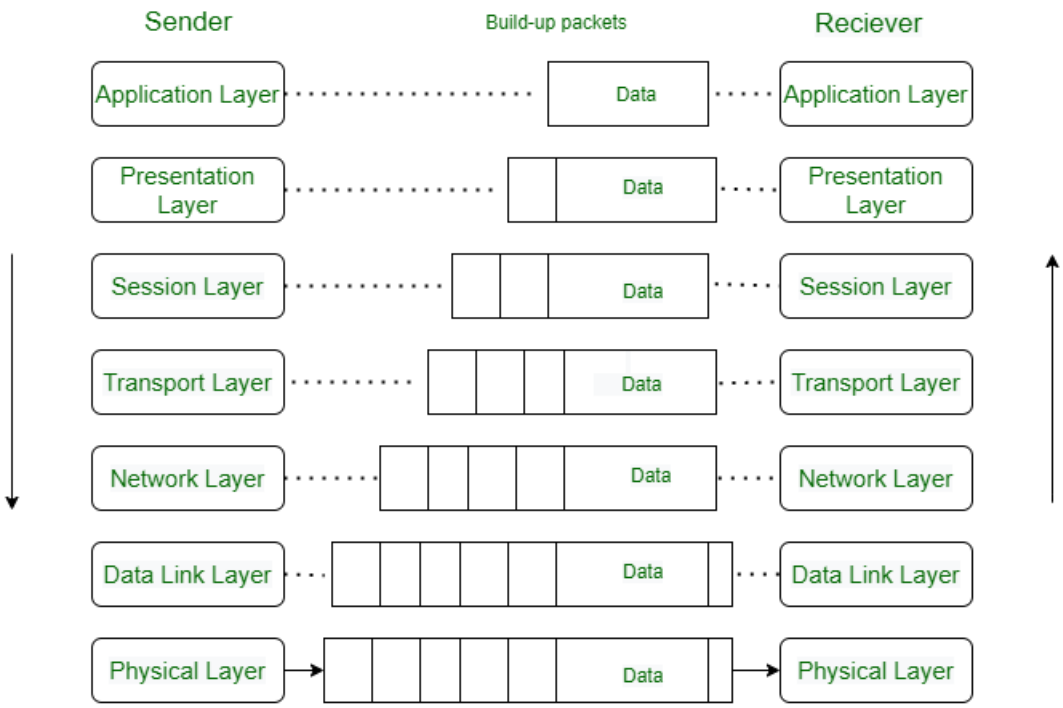


Рисунок 1.2 – Модель OSI Передача/Прийом

1.3 Сім рівнів моделі OSI.

Модель OSI складається з семи рівнів абстракції, розташованих у порядку зверху вниз:

1. Фізичний рівень
2. Канальний рівень даних
3. Мережевий рівень
4. Транспортний рівень
5. Рівень сесії
6. Рівень презентації
7. Рівень програми

Модель взаємозв'язку відкритих систем (OSI) описує сім рівнів, які комп'ютерні системи використовують для зв'язку через мережу. Це була перша стандартна модель мережевих комунікацій, прийнята всіма великими комп'ютерними та телекомунікаційними компаніями на початку 1980–х років.

Сучасний Інтернет базується не на OSI, а на простішій моделі TCP/IP. Проте 7–рівнева модель OSI все ще широко використовується, оскільки вона

допомагає візуалізувати та повідомити, як працюють мережі, а також допомагає ізолювати та вирішувати проблеми з мережею.

OSI був представлений у 1983 році представниками великих комп'ютерних і телекомунікаційних компаній і був прийнятий ISO як міжнародний стандарт у 1984 році.

1.4 Фізичний рівень – Рівень 1

Найнижчим рівнем еталонної моделі OSI є фізичний рівень. Він відповідає за фактичне фізичне з'єднання між пристроями. Фізичний рівень містить інформацію у формі бітів**.** Він відповідає за передачу окремих бітів від одного вузла до іншого. При отриманні даних цей рівень отримує отриманий сигнал і перетворює його на 0 і 1 і надсилає їх на рівень каналу даних, який збирає кадр назад.

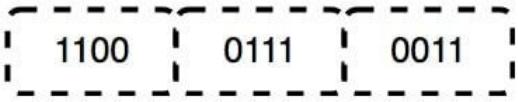


Рисунок 1.3 – Побітна структура пакету фізичного рівня моделі OSI

Функції фізичного рівня

- Синхронізація бітів: Фізичний рівень забезпечує синхронізацію бітів за допомогою синхронізації. Цей годинник контролює як відправника, так і отримувача, таким чином забезпечуючи синхронізацію на бітовому рівні.
- Контроль швидкості передачі: Фізичний рівень також визначає швидкість передачі, тобто кількість бітів, що надсилаються за секунду.
- Фізичні топології: Фізичний рівень визначає, як різні пристрої/вузли розташовані в мережі, тобто топологія шини, зірки або сітки.
- Режим передачі: Фізичний рівень також визначає, як дані передаються між двома підключеними пристроями. Можливі різні режими передачі: симплексний, напівдуплексний і повнодуплексний.

Примітка:

1. Концентратор, повторювач, модем і кабелі є пристроями фізичного рівня.
2. Мережний рівень, рівень каналу даних і фізичний рівень також відомі як нижні рівні або апаратні рівні .

1.5 Канальний рівень (DLL – DataLinkLayer) – рівень 2

Канальний рівень відповідає за доставку повідомлення від вузла до вузла. Основною функцією цього рівня є забезпечення безпомилкової передачі даних від одного вузла до іншого на фізичному рівні. Коли пакет надходить у мережу, DLL відповідає за його передачу на хост, використовуючи його MAC–адресу. Рівень каналу даних розділений на два підрівні:

1. Logical Link Control (LLC)
2. Контроль доступу до медіа (MAC)

Пакет, отриманий від мережевого рівня, далі ділиться на кадри залежно від розміру кадру NIC (карта мережевого інтерфейсу). DLL також інкапсулює MAC–адресу відправника та одержувача в заголовку.

MAC–адреса приймача отримується шляхом розміщення ARP–запиту (протоколу розпізнавання адрес) у дроті із запитом «Хто має цю IP–адресу?» і хост призначення відповість своєю MAC–адресою.

Функції канального рівня

- Кадрування: кадрування є функцією канального рівня. Він надає можливість відправнику передавати набір бітів, які мають значення для одержувача. Це можна зробити, прикріпивши спеціальні бітові шаблони до початку та кінця кадру.
- Фізична адресація: після створення кадрів канальний рівень додає фізичні адреси (MAC–адреси) відправника та/або одержувача в заголовок кожного кадру.
- Контроль помилок: Канальний рівень забезпечує механізм контролю помилок, у якому він виявляє та повторно передає пошкоджені або втрачені кадри.

- Контроль потоку: швидкість передачі даних має бути постійною з обох сторін, інакше дані можуть бути пошкоджені, тому керування потоком координує кількість даних, які можна надіслати до отримання підтвердження.
- Контроль доступу: коли один канал зв’язку використовується кількома пристроями, підрівень MAC канального рівня допомагає визначити, який пристрій контролює канал у певний момент часу.

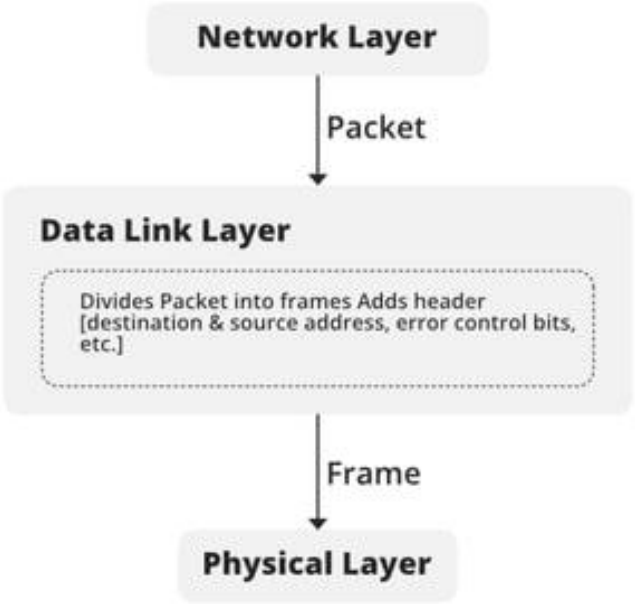


Рисунок 1.4 – Функції канального рівня еталонної моделі OSI

Примітка:

1. Пакет на рівні каналу даних називається кадром.
2. Канальний рівень обробляється NIC (картою мережевого інтерфейсу) і драйверами пристроїв хост–машин.
3. Комутатор і міст — це пристрої канального рівня.

1.6 Мережевий рівень – рівень 3

Мережевий рівень працює для передачі даних від одного хоста до іншого, розташованого в різних мережах. Він також піклується про маршрутизацію пакетів, тобто вибір найкоротшого шляху для передачі пакету з числа доступних маршрутів. IP–адреси відправника та одержувача розміщуються в заголовку на мережевому рівні.

Функції мережевого рівня

- Маршрутизація: протоколи мережевого рівня визначають, який маршрут підходить від джерела до пункту призначення. Ця функція мережевого рівня відома як маршрутизація.
- Логічна адресація: для однозначної ідентифікації кожного пристрою в Інтернеті мережевий рівень визначає схему адресації. IP–адреси відправника та одержувача розміщуються в заголовку на мережевому рівні. Така адреса виділяє кожен пристрій унікально та універсально.

Примітка:

1. Сегмент на мережевому рівні називається пакетом .
2. Мережевий рівень реалізується мережевими пристроями, такими як маршрутизатори та комутатори.

1.7 Транспортний рівень – рівень 4

Транспортний рівень надає послуги прикладному рівню та отримує послуги від мережевого рівня. Дані на транспортному рівні називаються *сегментами* . Він відповідає за наскрізну доставку всього повідомлення. Транспортний рівень також забезпечує підтвердження успішної передачі даних і повторно передає дані, якщо виявлено помилку.

На стороні відправника: транспортний рівень отримує відформатовані дані з верхніх рівнів, виконує сегментацію , а також реалізує контроль потоку та помилок для забезпечення належної передачі даних. Він також додає номери портів джерела та призначення у свій заголовок і пересилає сегментовані дані на мережевий рівень.

Примітка. Відправник повинен знати номер порту, пов’язаний із програмою одержувача. Зазвичай цей номер порту призначення налаштовується за замовчуванням або вручну. Наприклад, коли веб–програма запитує веб–сервер, вона зазвичай використовує номер порту 80, оскільки це

стандартний порт, призначений для веб–програм. Багато програм мають стандартні порти.

На стороні одержувача: транспортний рівень зчитує номер порту зі свого заголовка та пересилає дані, які він отримав, до відповідної програми. Він також виконує секвенування та повторне збирання сегментованих даних.

Функції транспортного рівня

- Сегментація та повторна збірка: цей рівень приймає повідомлення від рівня (сеансу) і розбиває повідомлення на менші блоки. Кожен із створених сегментів має пов’язаний із ним заголовок. Транспортний рівень на станції призначення повторно збирає повідомлення.
- Адресація точки обслуговування: щоб доставити повідомлення правильному процесу, заголовок транспортного рівня включає тип адреси, який називається адресою точки обслуговування або адресою порту. Таким чином, вказуючи цю адресу, транспортний рівень забезпечує доставку повідомлення до правильного процесу.

Послуги, що надаються транспортним рівнем

1. Сервіс, орієнтований на підключення
2. Сервіс без підключення

Сервіс, орієнтований на підключення, – це трифазний процес, який включає: встановлення підключення, передачу даних, припинення/відключення

У цьому типі передачі приймаючий пристрій надсилає підтвердження назад до джерела після отримання пакета або групи пакетів. Цей тип трансмісії надійний і безпечний.

Послуга без підключення, – це однофазний процес і включає передачу даних. У цьому типі передачі одержувач не підтверджує отримання пакету. Такий підхід забезпечує набагато швидший зв’язок між пристроями. Сервіс, орієнтований на з’єднання, надійніший, ніж сервіс без з’єднання.

Примітка:

1. Дані на транспортному рівні називаються сегментами.

2. Транспортний рівень управляється операційною системою. Він є частиною ОС і зв’язується з прикладним рівнем за допомогою системних викликів.
3. Транспортний рівень називається серцем моделі OSI.
4. Використання пристрою або протоколу: TCP, UDP NetBIOS, PPTP

1.8 Рівень сеансу – Рівень 5

Цей рівень відповідає за встановлення з'єднання, підтримку сеансів і аутентифікацію, а також забезпечує безпеку.

Функції сеансового рівня

- Встановлення, підтримка та завершення сеансу: рівень дозволяє двом процесам встановлювати, використовувати та завершувати з’єднання.
- Синхронізація: цей рівень дозволяє процесу додавати контрольні точки, які вважаються точками синхронізації в даних. Ці точки синхронізації допомагають визначити помилку, щоб дані було повторно синхронізовано належним чином, а кінці повідомлень не обрізалися передчасно та уникали втрати даних.
- Контролер діалогу: Рівень сеансу дозволяє двом системам почати зв’язок одна з одною в напівдуплексному або повному дуплексному режимі.

Примітка:

1. Усі наведені нижче 3 рівні (включаючи сеансовий рівень) інтегровані як єдиний рівень у модель TCP/IP як «рівень додатків».
2. Реалізація цих 3 рівнів виконується самим мережевим додатком. Вони також відомі як верхні рівні або програмні рівні.
3. Використання пристрою або протоколу: NetBIOS, PPTP.

Давайте розглянемо сценарій, коли користувач хоче надіслати повідомлення через якусь програму Messenger, запущену в його браузері. «Месенджер» тут діє як прикладний рівень, який надає користувачеві інтерфейс для створення даних. Це повідомлення або так звані Дані стискаються,

шифруються (якщо є безпечні дані) і перетворюються на біти (0 і 1), щоб їх можна було передати.

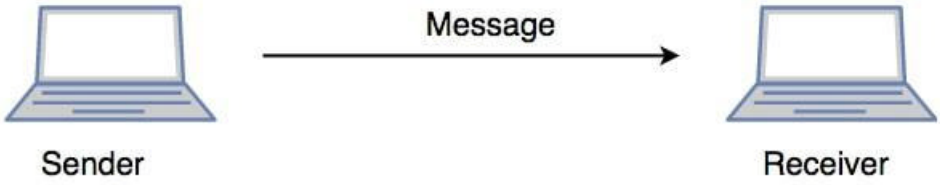


Рисунок 1.5 – Зв'язок на сеансовому рівні еталонної моделі OSI

1.9 Рівень презентації – Рівень 6

Рівень презентації також називають рівнем перекладу . Тут витягуються дані з прикладного рівня та обробляються відповідно до необхідного формату для передачі через мережу.

Функції рівня презентації

- Переклад: наприклад, ASCII в EBCDIC.
- Шифрування/дешифрування: шифрування даних перетворює дані в іншу форму або код. Зашифровані дані називаються зашифрованим текстом, а розшифровані — звичайним текстом. Значення ключа використовується як для шифрування, так і для дешифрування даних.
- Стиснення: зменшує кількість бітів, які необхідно передати в мережі.

Примітка. Використання пристрою чи протоколу: JPEG, MPEG, GIF

1.10 Рівень програми – Рівень 7

На самому верху стеку рівнів еталонної моделі OSI ми знаходимо прикладний рівень, який реалізується мережевими програмами. Ці програми виробляють дані, які потрібно передати через мережу. Цей рівень також служить вікном для доступу служб програми до мережі та для відображення отриманої інформації користувачеві.

Приклад : програма – браузери, Skype Messenger тощо.

Примітка:

1. Рівень програми також називається рівнем робочого столу.

2. Використання пристрою або протоколу: SMTP

Функції прикладного рівня

Основні функції прикладного рівня наведені нижче.

- Мережевий віртуальний термінал: дозволяє користувачеві увійти на віддалений хост.
- FTAM – доступ до передачі файлів і керування ними: ця програма дозволяє користувачеві отримувати доступ до файлів на віддаленому хості, отримувати файли на віддаленому хості та керувати або контролювати файли з віддаленого комп’ютера.
- Поштові послуги: надання послуг електронної пошти.
- Служби каталогів: ця програма надає джерела розподілених баз даних і доступ до глобальної інформації про різні об’єкти та служби.

Примітка. Модель OSI діє як еталонна модель і не реалізована в Інтернеті через пізній винахід. Поточна використовується модель TCP/IP.

1.12 Узагальнення моделі OSI.

№ шару	Назва шару	Відповідальність	Інформаційна форма (блок даних)	Пристрій або протокол
7	Рівень програми	Допомагає в ідентифікації клієнта та синхронізації зв'язку.	повідомлення	SMTP
6	Рівень презентації	Дані з прикладного рівня витягуються та обробляються в необхідному форматі для передачі.	повідомлення	JPEG, MPEG, GIF
5	Рівень сесії	Встановлює підключення, технічне обслуговування, забезпечує автентифікацію та забезпечує безпеку.	повідомлення	Шлюз
4	Транспортний рівень	Візьміть послугу з мережевого рівня та надайте її прикладному рівню.	Відрізок	Брандмауер
3	Мережевий рівень	Передача даних від одного хоста до іншого, розташованого в різних мережах.	пакет	Маршрутизатор
2	Канальний рівень даних	Доставка повідомлення від вузла до вузла.	рамка	Перемикач, міст
1	Фізичний рівень	Встановлення фізичних з’єднань між пристроями.	біти	Хаб, ретранслятор, модем, кабелі

1.13 Порівняння моделі OSI та TCP/IP

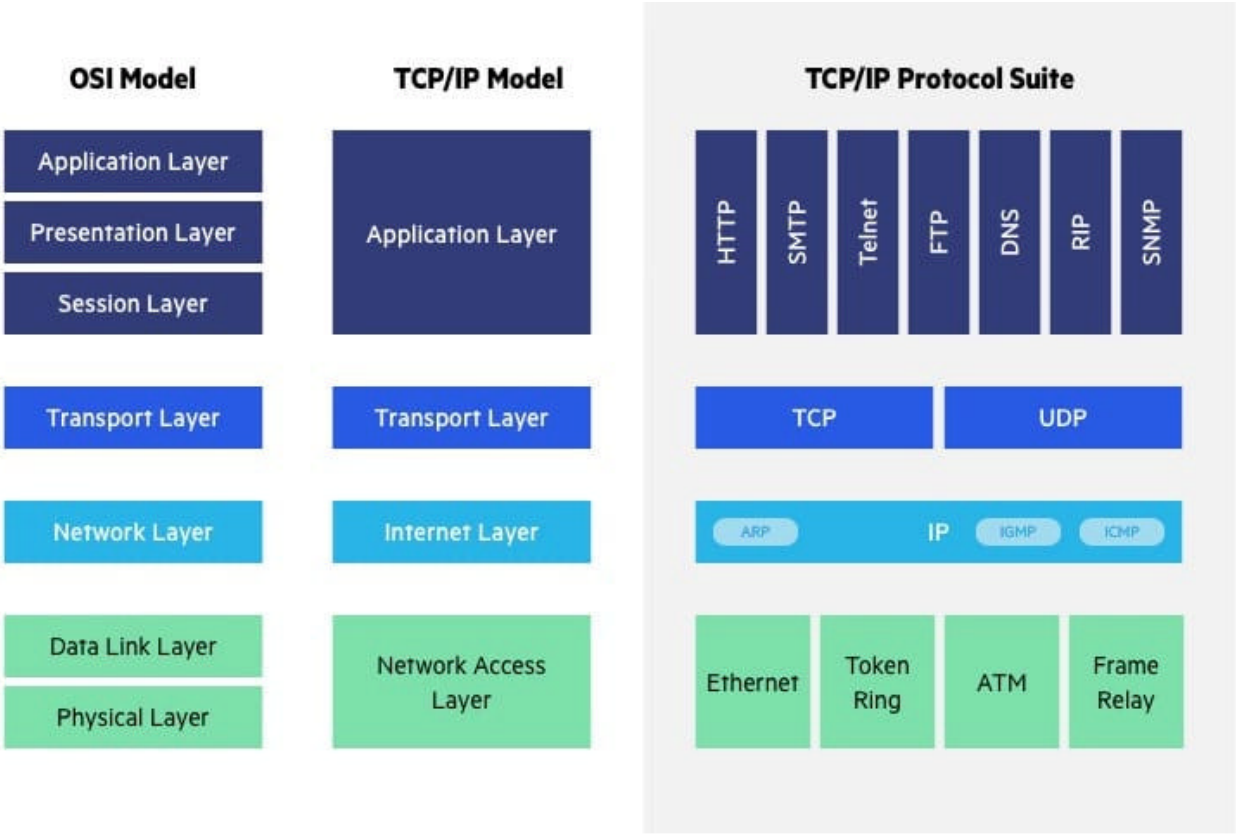


Рисунок 1.6 – Порівняння моделі OSI та TCP/IP

Протокол управління передачею/інтернет–протокол (TCP/IP) є старшим за модель OSI. Він був створений Міністерством оборони США (DoD).

Ключова відмінність між моделями полягає в тому, що TCP/IP є простішим, оскільки кілька рівнів OSI згортаються в один:

- Рівні OSI 5, 6, 7 об’єднані в один прикладний рівень у TCP/IP
- Рівні OSI 1, 2 об’єднані в один рівень мережевого доступу в TCP/IP, однак TCP/IP не бере на себе відповідальності за функції послідовності та підтвердження, залишаючи їх базовому транспортному рівню.

Інші важливі відмінності:

- TCP/IP — це модель функціональна, призначена для рішення проблем зв’язку, яка базується на певних стандартних мережевих протоколах. OSI – це загальна, незалежна від протоколів модель, призначена для опису всіх форм мережевого зв’язку.

- У TCP/IP програми, як правило, використовують усі рівні, тоді як в OSI прості програми не використовують усі рівні. Лише рівні 1, 2 та 3 є обов'язковими для забезпечення будь–якої передачі даних.

Рішення безпеки в мережевих з'єднаннях захищають ваші додатки на кількох рівнях моделі OSI, від мережевого рівня, захищеного пом'якшенням DDoS–атак, до брандмауера веб–додатків (WAF), керування ботами та технології безпеки API , які захищають прикладний рівень.

Щоб захистити додатки та мережі через стек OSI, забезпечується багаторівневий захист, щоб веб–сайти та додатки були доступними, легко доступними та безпечними.

Рішення безпеки по рівнях моделі OSI включає:

- Захист від DDoS — підтримка безвідмовної роботи в будь–яких ситуаціях. Запобігання будь–якому типу DDoS–атак будь–якого розміру, щоб запобігти доступу до веб–сайту та мережевої інфраструктури.
- CDN – підвищує продуктивність веб–сайтів та зменшує витрати на пропускну здатність за допомогою CDN, він кешує статичні ресурси на межі, одночасно прискорюючи API та динамічні веб–сайти.
- WAF — хмарне рішення дозволяє легітимний трафік і запобігає поганому трафіку, захищаючи програми на межі. Шлюз WAF забезпечує безпеку програм і API у мережі.
- Захист від ботів — аналізує трафік бота, щоб виявити аномалії, виявляє погану поведінку ботів і перевіряє її за допомогою механізмів перевірки, які не впливають на трафік користувачів.
- Безпека API — захищає API, забезпечуючи доступ лише бажаного трафіку до кінцевої точки API, а також виявляючи та блокуючи використання вразливостей.

- Захист від захоплення облікових записів – використовує процес виявлення на основі намірів для ідентифікації та захисту від спроб захоплення облікових записів користувачів із зловмисною метою.
- RASP – захищає програми зсередини від відомих атак і атак нульового дня. Швидкий і точний захист без підпису або режиму навчання.
- Аналітика атак – ефективно й точно зменшує реальні загрози кібербезпеки та реагує на них за допомогою оперативної інформації на всіх рівнях захисту.

2 ТЕХНОЛОГІЧНА ЧАСТИНА

2.1 Протоколи доступу до середовища по рівнях моделі OSI.

Ілюстрація канального рівня із забезпечення сервісу мережевого рівня представлена на рис. 2.1. Призначення цього сервісу – допомогти передати дані процесу на мережевому рівні однієї машини процесу на мережевий рівень іншої машини.

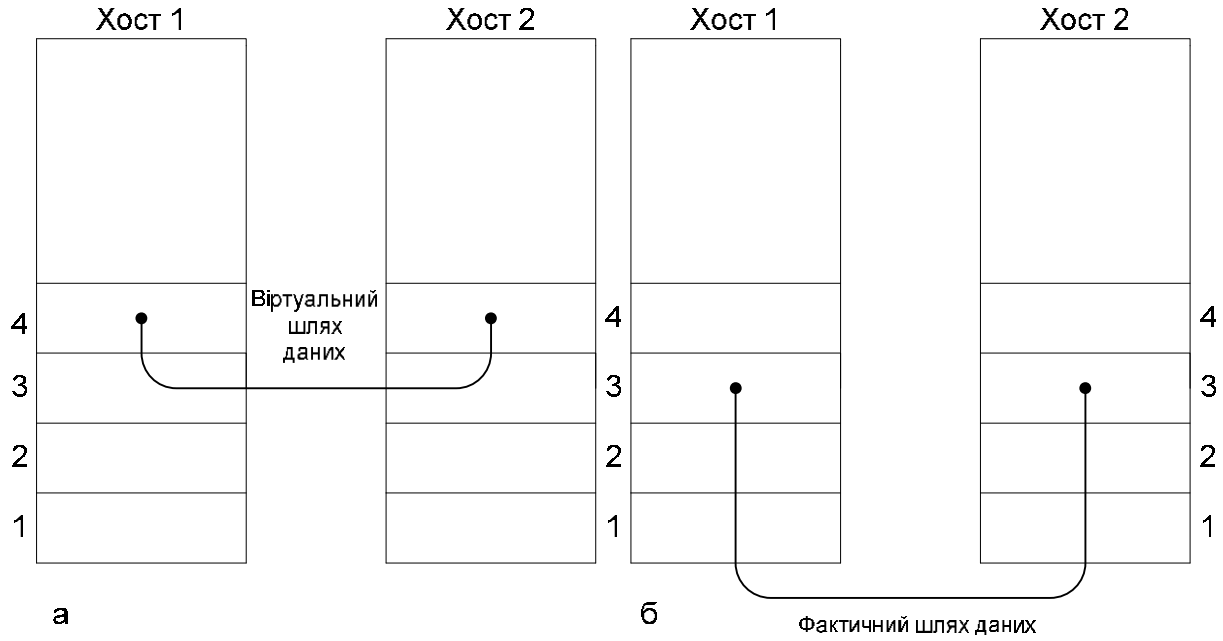


Рисунок 2.1 – Віртуальне з'єднання (а); реальне з'єднання (б)

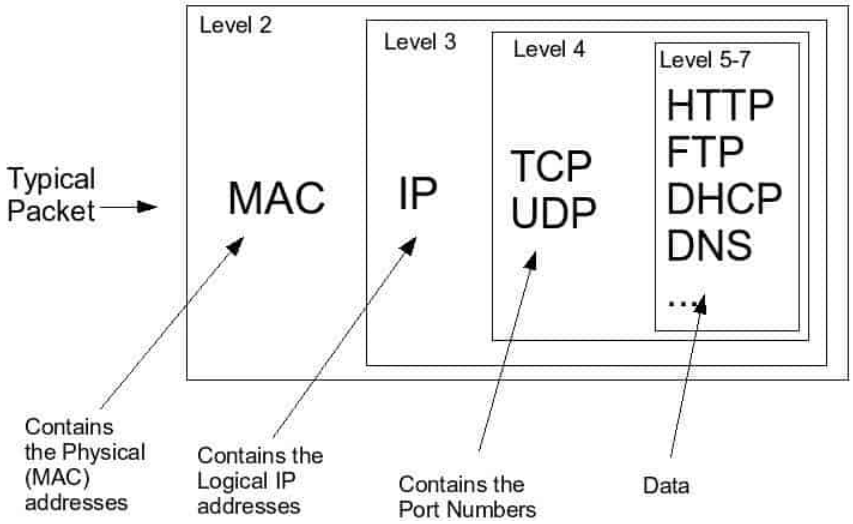


Рисунок 2.2 – Формат мережевого пакета даних по рівнях і протоколах моделі OSI

Передачу даних згідно рівнів моделі OSI показано на рис 2.1. Фактична передача даних відбувається як показано на 2**Ошибка! Источник ссылки не найден.**.1 b. Однак, для простоти будемо вважати, що це відбувається як на рис. 2.1a. На рис. 2.2 зображено формат мережевого пакета даних у відповідності до рівнів моделі OSI і мережевих протоколів, котрі використовуються на даних рівнях.

Безпосередньо передачу даних ілюструє рис. 2.3.

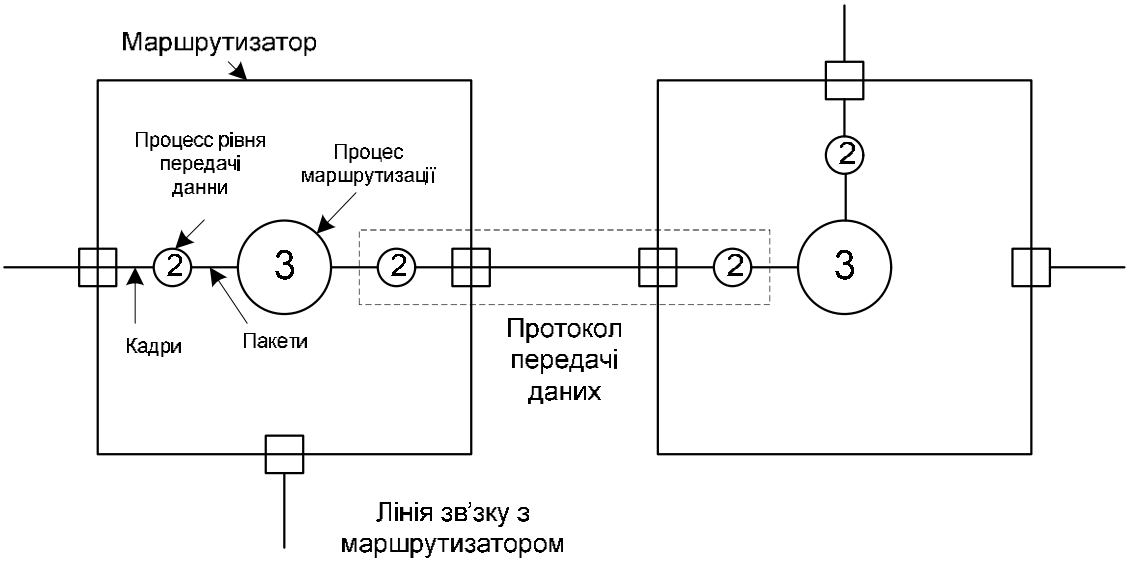


Рисунок 2.3 – Протокол передачі даних

На рис. 2.3 показано типовий фрагмент WAN де два маршрутизатори з'єднані через телефонну лінію. Коли кадр надходить у маршрутизатор, апаратура перевіряє контрольну суму й передає кадр канальному рівню. Канальний рівень перевіряє чи є кадр, що надійшов, очікуваним і якщо так, то передає пакет, розташований у кадрі, мережевому рівню на іншій машині. Процес на мережевому рівні вибирає належну лінію для передачі й посилає пакет на канальний рівень.

Не бажано на мережевому рівні займатися пропажею кадрів. Це завдання канального рівня забезпечити надійний канал. Це особливо важливо при бездротовому середовищі передачі.

2.2 Розбивка на кадри та виявлення помилок.

Сервіс, створюваний канальним рівнем моделі OSI для мережевого, реалізований на сервісі, котрий створюється фізичним рівнем. Саме на фізичному рівні відбувається потокова фізична передача бітів інформації. Послана кількість біт інформації не завжди дорівнює прийнятій, значення відправленого біта не завжди дорівнює прийнятому, що означатиме помилку передачі. Відповідно на канальному рівні потрібно забезпечити протоколи і алгоритми по виявленню й виправленню помилок.

Рішення даної проблеми це розбивка потоку біт на кадри, визначення контрольної суми кожного кадру при пересиланні даних.

При прийманні контрольна сума рахується для кожного кадру і порівнюється з тою, що збережена у кадрі. Якщо суми відрізняються, це означає помилку передачі. Канальний рівень забезпечує виправлення помилок, скидає ушкоджений кадр, відсилає інформацію про помилку відправнику цього кадру, так як у кадрі крім контрольної суми міститься інформація про його призначення.

Розбивка потоку бітів на кадри завдання не просте. Один зі способів – робити часову паузу між бітами різних кадрів. Однак, у мережі де немає єдиного таймера немає гарантії, що ця пауза зберегтися або, навпаки, не з'являться нові.

Часові методи ненадійні, тому застосовуються інші. Розглянемо чотири основних:

- лічильник символів
- вставка спеціальних стартових і кінцевих символів
- вставка стартових і кінцевих бітів
- порушення кодування на фізичному рівні

Перший метод показаний на рис 2.4. У початок кожного кадру вказується скільки символів у кадрі. При прийманні число прийнятих символів підраховується знову. Однак, цей метод має істотний недолік: лічильник

символів може бути перекручений при передачі. Тоді приймаюча сторона не зможе виявити границі кадру. Навіть виявивши помилку контрольних сум, що приймаються, сторона не зможе повідомити відправнику який кадр потрібно переслати, скільки символів пропало. Цей метод сьогодні використовується рідко.

Рисунок 2.4 – Потік символів: без помилок (а); з однією помилкою (б)

Другий метод побудований на вставці спеціальних символів. Звичайно для цього використовують аж послідовність DLE_STX для початку кадру й DLE_ETX для кінця кадру. DLE – Data_Link_Escape; STX – Start_TeXt, ETX – End_TeXt. При цьому методі якщо навіть була загублена границя поточного кадру, треба просто шукати найближчу послідовність DLE_STX або DLE_ETX. Тут існує небезпека: при передачі чисел або програми в об'єктному коді такі послідовності можуть уже втримуватися в переданих даних. Для рішення цієї проблеми використовується прийом екранування: кожна послідовність DLE просто дублюється в переданих даних. Тому при прийманні якщо є два послідовних DLE, те один віддаляється. Цей метод проілюстрований на Рис. 2.5.

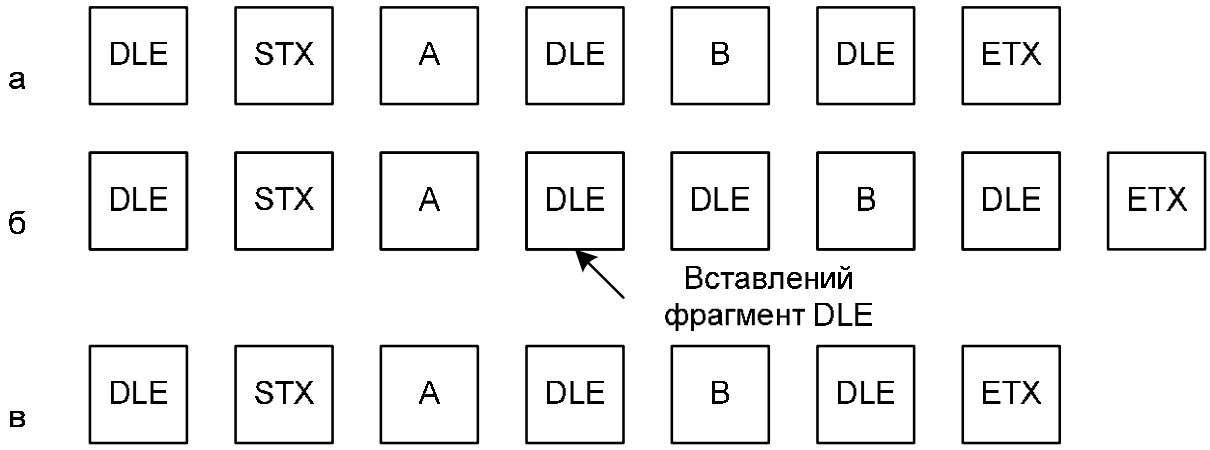


Рисунок 2.5 Кадр, обмежений діалоговими байтами (а); кадр, оброблений на канальному рівні (б); дані, передані на мережевий рівень (в)

Основним недоліком цього методу є те, що він жорстко пов'язаний з розміром байта й кодуванням ASCII. У міру розвитку мереж цей зв'язок ставав усе більше й більше обтяжливим.

Був запропонований новий прийом, що дозволяє використовувати будь–яке число бітів на символ і будь–яке кодування. Його ідея полягає в тому, що кожний кадр починається й закінчується зі спеціального прапор–байта: 01111110, – сторона, що його посилає, зустрівши послідовно 5 одиниць обов'язково вставить 0. Приймаюча сторона, прийнявши 5 послідовних одиниць обов'язково видалить наступний за ними 0. Якщо в переданих даних зустрінеться конфігурація прапор–байта, то вона буде перетворена в конфігурацію 011111010. Цей метод ілюструє рис. 2.6. Він прозорий для мережевого рівня так само як і метод вставки байтів.

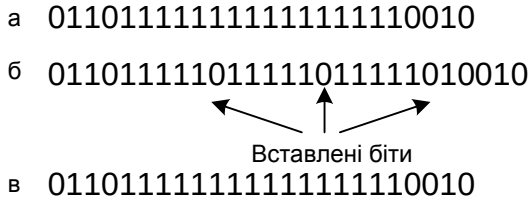


Рисунок 2.6 – Бітове заповнення: вихідні дані (а); дані на лінії (б); дані, збережені в пам'яті після видалення вставлених бітів (в)

Таким чином, кадр легко може бути розпізнаний по прапор–байту. Якщо границя чергового кадру з якоїсь причини була загублена, то потрібно відстежити найближчий прапор–байт.

Останній метод використовується там, де застосовується спеціальне кодування бітів на фізичному рівні. Наприклад, для передачі одного біта використовується два імпульси. 1 кодується як перехід високий–низький рівень, 0 – як низький–високий рівень. Сполучення низьке–низьке або високе–високе не використовуються для передачі даних. Їх використовують для границь кадру. Так передача реалізована у стандарті IEEE 802 для LAN.

Нарешті, на практиці використовують, як правило, комбінацію цих методів. Наприклад, лічильник символів з одним з вище перерахованих. Тоді якщо число символів у кадру збігається з кодуванням границі кадру, кадр вважається переданим правильно.

2.3 Керування потоком

Іншою важливою проблемою, що виникає на канальному рівні це керування потоком. Справа в тому, може цілком трапитися, що відправник буде вислати кадри настільки часто, що одержувач не буде встигати їх обробляти. Це може трапитися якщо, наприклад, машина–відправник потужніша або завантажена слабкіше, ніж машина–одержувач.

Для боротьби з такими ситуаціями вводять керування потоком. Це керування припускає зворотний зв'язок між відправником і одержувачем, що дозволяє їм урегулювати такі ситуації. Є багато схем керування потоком, але всі вони в основі своєї використовують наступний сценарій.

Перш ніж відправник почне передачу він запитує в одержувача скільки кадрів той може прийняти. Одержувач повідомляє його певне число кадрів. Відправник після того як передасть це число кадрів, повинен призупинити передачу й запитати одержувача знову одержувача знову як багато кадрів той

може прийняти й т.д. Пізніше на конкретних прикладах ми познайомимося з конкретними механізмами керування потоком.

2.4 Коди з виправленням помилок

Для надійної передачі побітних даних на канальному рівні запропоновано два методи. Перший – вносять надмірність у формі додаткових бітів у переданий блок даних так, щоб аналізуючи отриманий блок, можна було би виявити місце помилки. Це є коди з виправленням помилок. Другий – вносять надмірність, але лише стільки, щоб, згідно аналізу отриманих даних можна було зробити висновок є в переданому блоці помилки чи відсутні. Це впроваджені коди виявлення помилок.

Нехай дані займають m розрядів і ми додаємо r розрядів як контрольні розряди. Нам треба передати слово довжиною n, що називають n–бітовим кодових словом. Нехай у нас є два кодових слова 10001001 і 10110001. За допомогою операції EXCLUSIVE OR легко визначити число різних розрядів. У цьому випадку їх 3. Кількість різних бітів у двох кодових словах називається відстанню Хеммінга. Тому якщо два кодових слова перебувають на відстані d по Хеммінгу, це значить, що треба перетворити рівно d розрядів, щоб перетворити одне кодових слово в інше.

У силу надмірності не всі 2^n комбінацій можливі. Знаючи алгоритм установки контрольних розрядів, ми можемо обчислити мінімальну відстань по Хеммінгу між припустимими кодовими словами. Здатний код виправляти помилки або тільки виявляти залежить від відстані між його кодовими словами по Хеммінгу. Якщо ми хочемо виявляти d помилок, то треба щоб кодові слова розміщувались одне від одного на відстані $d+1$. Тоді якщо прийнятий код розміщений на відстані $k<d$, тобно прийняте кодове слово містить k помилок. Якщо ми хочемо виправляти помилки, то потрібно щоб кодові слова розміщувались одне від одного на відстані $2d+1$. Тому якщо передане кодове

слово містить d помилок, воно однаково ближче до правильного кодового слова чим до будь якого іншого, отже можна визначити, вихідне слово.

Прикладом коду визначення однієї помилки є код з бітом парності. Його конструкція наступна, – до вихідного кодового слова додають біт парності. Якщо число 1 у вихідному кодовому слові парне, то відповідно значення цього біту – 0. Якщо непарне, то 0. Кодові слова з бітом парності мають відстань Хеммінга – 2.

Для прикладу розглянемо код, у якого є тільки чотири правильних кодових слова: 0000000000, 0000011111, 11111100000, 11111111111. Відстань по Хеммінгу в цього коду 5, тобно він може виправляти подвійні помилки. Якщо одержувач одержить слово 0000000111, то зрозуміло, що вихідне слово мало вигляд 0000011111 .

Визначимо мінімальну кількість контрольних розрядів, необхідних для виправлення одиночних помилок. Нехай у нас є код з $m-$ бітів повідомлення й $n-$ контрольних бітів. Кожне із 2^m правильних кодових слів містить 2^n неправильних кодових слів на відстані 1. Такими чином, з кожним з 2^m кодових слів пов'язано $n+1$ кодових слів. Тому що загальне число кодових слів 2^n, тобто $(n+1)2^m \le 2^n$, з огляду на що $n=m+r$ одержуємо $(m+r+1)\le 2^r$.

Ця теоретична межа досяжна при використанні методу, запропонованого Хеммінгом.

Код Хеммінга виправляє тільки одиничні помилки. Однак є методи, що дозволяє поширити алгоритм Хеммінга на випадки групових помилок.

Для прикладу, нехай у нас є канал з одиничними помилками із частотою 10–6 на біт. Якщо ми хочемо виправляти одиничні помилки при передачі блоку в 1000 біт, то нам буде потрібно 10 контрольних біт. При передачі 1 Мбіт даних, буде потрібно 10000 контрольних біт. У той же час для виявлення одиничної помилки досить одного біта парності. Тому, якщо ми застосуємо техніку повторної передачі, то на передачу 1000 блоків потрібно буде

витратити 1001 біт додатково або з повторною передачею 2002 біта, замість 10000 біт у випадку коду з виправленням помилки.

Застосування техніки парності "у лоб" у випадку групових помилок не дасть потрібного результату. Однак, її можна скорегувати. Нехай нам треба передати n слів по k біт. Розташуємо їх у вигляді матриці nk. Для кожного стовпця обчислимо біт парності й розмістимо його в додатковому рядку. Матриця потім передається по рядках. По одержанню матриця відновлюється і якщо хоч один біт порушений, то весь блок передається повторно.

Цей метод дозволяє виявити групові помилки довжини n. Проти групових помилок довжини $n+1$ він неспроможний. У загальному випадку ймовірність правильної передачі при довжині груповій помилці n, дорівнює 2^{-n}.

Тому на практиці застосовують іншу техніку, що називається поліноміальними кодами або циклічним надлишковим кодом (Cyclic Redundancy Code) або CRC кодом.

CRC коди побудовані на розгляді бітового рядка як рядка коефіцієнтів полінома. k бітовий рядок – коефіцієнти полінома ступеня $k-1$. Самий лівий біт рядка – коефіцієнт при старшому ступені. Наприклад, рядок 110001 представляє поліном $x_5 + x_4 + x_0$.

Поліноміальна арифметика виконується по модулю 2. Додавання й вирахування відбувається без переносу розрядів. Так що ці обидві операції еквівалентні EXCLUSIVE OR. Наприклад,

10011011	00110011	01010101	11110000
+	+	-	-
11001010	10011011	10101111	10100110
01010001	11111110	11111010	01010110

Розподіл виконується як звичайно у двійковій системі з тією лише різницею, що розрахунок виконується по модулю два.

Використання поліноміальних кодів при передачі полягає в наступному. Відправник і одержувач заздалегідь домовляються про конкретний генератор

поліномів $G(x)$, у нього коефіцієнти при старшому члені й при молодшому члені повинні бути рівні 1. Нехай ступінь $G(x)$ дорівнює r. Для обчислення контрольної суми блоку з m біт треба щоб обов'язково $m>r$. Ідея полягає в тому, щоб додати контрольну суму до переданого блоку, розглянутому як поліном $M(x)$ так, щоб переданий блок з контрольною сумою був кратний $G(x)$. Коли одержувач одержує блок з контрольною сумою, він ділить його на $G(x)$. Якщо є залишок, то були помилки при передачі.

Алгоритм обчислення контрольної суми:

1) Додати r нулів у кінець блоку так, що він тепер містить m+r розрядів і відповідає поліному $x^r M(x)$;
2) Розділити по модулю 2 поліном $x^r M(x)$ на $G(x)$;
3) Відняти залишок (довжина якого завжди не більше r розрядів) з рядка, що відповідає $x^r M(x)$, по модулю 2. Результат і є блок з контрольною сумою (назвемо його $T(x)$).

Цей метод дозволяє відловлювати одиночні помилки. Групові помилки довжини не більше r. Непарне число окремих помилок.

Існує три міжнародних стандарти на вид $G(x)$:

$$\text{CRC-12} = x^{12} + x^{11} + x^3 + x^2 + x + 1$$

$$\text{CRC-16} = x^{16} + x^{15} + x^2 + 1$$

$$\text{CRC-CCITT} = x^{16} + x^{12} + x^5 + 1.$$

CRC–12 використовується для передачі символів з 6 розрядів. Два інших – для 8 розрядних. CRC–16 і CRC–CCITT ловлять одиночні, подвійні помилки, групові помилки довжиною не більше 16 і непарне число ізольованих помилок з імовірністю 99,997%.

2.5 Доступ до середовища, моделі статичного й динамічного виділення каналу.

Будемо розглядати протоколи доступу до фізичного середовища передачі даних із множинним доступом. Існує два види середовищ передачі даних: крапка–крапка та із множинним доступом. У середовищі крапка–крапка доступ можливий тільки із двох сторін. Проблеми синхронізації доступу тут не настільки складні. Цей вид середовищ передачі характерний для WAN мереж. Тут ми розглянемо канали із множинним доступом або, як їх ще називають, протоколи з випадковим доступом.

У середовищах із множинним доступом ключовим виникає питання, – як визначити кому із абонентів, що дали запит на доступ, віддати канал. Для прикладу, розглянемо конференцію по телефону. Коли розмовник закінчить мову, то можливо, що відразу кілька учасників захочуть висловитися. Вони почнуть говорити одночасно. Як уникнути такої ситуації та запобігти хаосу. Саме протоколи для вирішення цієї проблеми розглянемо в подальшому.

Протоколи для визначення хто захопить канал у випадку конкуренції стосуються підрівня канального рівня, що називається MAC – Medium_Access_Control.

Основне питання, яке ми тут розглянемо – як розподіляти єдиний канал між багатьма конкуруючими користувачами.

2.5.1 Статичне надання каналу

Існує два основних підходи до поділу декількох конкуруючих користувачів на одному каналі – частотний поділ (Frequency–Division Multiplexing, FDM). Частотний поділ добре працює в умовах, коли число користувачів фіксоване і кожний абонент забезпечує щільне завантаження каналу. Тоді кожному з них виділяється своя смуга частот, котру він використовує незалежно від інших.

Однак, коли число користувачів велике або величина змінна, або коли трафік дуже не регулярний, в FDM з'являються проблеми. Якщо весь діапазон розділити на N смуг, тоді лише не багатьом з числа N буде потрібна передача, відповідно більша частина пропускної здатності буде губитися. Якщо число користувачів, кому необхідно передати дані, буде більше N, тоді частина з них одержить відмову через недостачу пропускної здатності, хоча частина тих кому канал буде наданий може нічого не передавати або не приймати.

У такий спосіб, припущення про сталість числа користувачів у середньому й статичному поділі каналу на підканали є не ефективним рішенням. Це твердження збільшує та обставина, що трафік у мережах, як правило, носить вибухоподібний характер (відмінність пікових навантажень від середніх досягає 1000 разів). Тому статичний розподіл був би не ефективний, тому що більшу частину часу канал простоював.

Це можна показати теоретично на наступній моделі. Нехай у нас є канал зі швидкістю C bps і ми хочемо оцінити середній час затримки T. Середня швидкість надходження кадрів дорівнює λ кадр/сек і середня довжина кадру має експонентний розподіл із середнім $1/\mu$ біт/кадр. Тоді

$$T = \frac{1}{\mu C - \lambda}$$

Тепер розділимо канал на N підканалів кожний зі швидкістю C/N bps. Швидкість надходження кадрів у кожному з підканалів буде тепер μ/N. Відповідно одержуємо

$$T_{\text{FDM}} = \frac{1}{\mu(C/N) - (\lambda/N)} = \frac{N}{\mu C - \lambda} = NT .$$

Звідси видно, що частотний поділ у N раз гірший, у порівнянні з тим як якби всі кадри якось були б розподілені з єдиної черги.

Ті ж самі міркування можна застосувати до часового поділу. Якщо кожному користувачеві виділити свій слот і той його не використовує, то це порожня витрата пропускної здатності каналу. Таким чином, жоден з відомих

статичних методів не дозволяє ефективно розподіляти навантаження. Тому ми зосередимося на динамічних методах.

2.5.2 Динамічне надання каналу

Перш ніж перейти до опису численних динамічних способів надання каналу сформулюємо основні п'ять припущень, які ми будемо використовувати:

- **Багатостанційна модель**. Модель складається з N незалежних станцій (комп'ютерів, телефонів, факс–машин і т.п.). На кожній працює користувач або програма, які генерують кадри для передачі. Імовірність, появи кадру в інтервалі $[t_1,t_2]$ дорівнює $\lambda(t_2-t_1)$, де ν константа. Передбачається, що якщо кадр згенерований, то новий не з'явиться, поки не буде переданий перший.
- **Модель єдиного каналу.** Канал один і він доступний всім станціям. Всі станції рівноправні. Вони одержують кадри й передають кадри тільки через цей єдиний канал. Апаратні засоби всіх станцій для доступу до каналу однакові, але програмно можна встановлювати пріоритети.
- **Модель із колізіями**. Якщо дві станції передають кадри в той саме час, то сигнали накладаються й руйнуються. Цей випадок будемо називати колізією. Будь–яка станція може виявити колізію. Кадри, що зштовхнулися в колізіями, повинні бути послані повторно пізніше. Крім колізій інших помилок передачі немає.
- **Часові моделі**:
  - ***Безперервний час***. Передача кадру може початися в будь–який момент. Немає єдиних годин у системі, які розбивають час на слоти.
  - ***Дискретний час***. Час розбивається на дискретні інтервали – слоти. Кадр починає передаватися тільки на початку слота. Слот може відповідати декільком кадрам, якщо це слот очікування, він може містити колізію, або успішну передачу.
- **Моделі з несучою**:
  - ***Виявлення несучої***. Станція завжди визначає зайнятий канал перш, ніж

використовувати його. Якщо він зайнятий, то жодна станція не починає передачу.

- ***Відсутність несучої.*** Станція нічого не знає про стан канал поки не почне використовувати його. Вона відразу починає передачу й лише пізніше виявляє колізію.

Перше припущення означає, що станції незалежні й на кожній працює тільки одна програма або користувач. Є й більше складні моделі. Єдиний канал передачі – це фундаментальне припущення. Немає іншого способу передати кадр – тільки по каналу. Стосовно часу може бути використано одне із двох припущень. Також мережа може використовувати припущення про виявлення несучої, а може його не використовувати.

2.6 Протоколи множинного доступу до каналів.

2.6.1 Сімейство протоколів ALOHA.

В 70–х роках Норман Абрамсон зі своїми колегами з університету Гаваї запропонував простий спосіб розподілу каналу. Абрамсон назвав систему ALOHA (це вітання по гавайськи), що складалася з наземних радіостанцій зв’язку, що зв'язують острови між собою. Ідея була дозволити у передавальному середовищі будь–якій кількості користувачів неконтрольовано використовувати той самий канал.

Ми тут розглянемо два варіанти системи: чиста ALOHA і слотована, тобто розбита на слоти. Основне розходження – у першому випадку ніякої синхронізації користувачів не потрібно, у другому вона потрібна.

2.6.2 Чиста ALOHA

Алгоритм чистої ALOHA простий – будь–який користувач намагається передати повідомлення. Завдяки тому, що у передавальному середовищі він завжди має зворотний зв'язок, то він спостерігає виникнення конфлікту при передачі. Цей зворотний зв'язок у середовищі LAN відбувається практично

миттєво (TTL), у системах супутникового зв'язку затримка становить близько 270 мсек.

Після виявлення конфлікту, користувач очікує деякий випадковий відрізок часу після чого здійснює повторну спробу передачі. Очікування має бути випадковим,в іншому випадку конкуренти будуть повторювати спроби в той самий час, що приведе до блокування.

Системи подібного типу, де користувачі конкурують за одержання загального каналу, називаються системами зі змаганнями. Неважливо, коли відбувся конфлікт, коли перший біт одного кадру наклався на останній біт іншого кадру або якось інакше, обидва кадри вважаються зіпсованими й повинні бути передані повторно. Контрольна сума не дозволяє розрізняти різні випадки накладення.

Яка ефективність системи ALOHA. Яка частина кадрів уникла колізій. Розглянемо наступну модель. Є необмежене число користувачів, що працюють на комп'ютерах. Все, що вони можуть робити це – або набирати текст, або чекати поки набраний текст передається. Коли користувач закінчує набирати черговий рядок, він зупиняється й чекає відповіді від системи. Система намагається передати цей рядок. Коли вона зробить це успішно, користувач бачить відгук і може продовжувати роботу.

Назвемо часом кадру – час необхідний на передачу кадру стандартної фіксованої довжини. Припускаємо, що користувачів не обмежене число й вони породжують кадри за законом Пуассона із середнім значенням S кадрів за час кадру. Оскільки при $S>1$ то черга на передачу буде тільки рости й всі кадри будуть страждати від колізій, то ми будемо припускати, $0<S<1$.

Також будемо припускати що ймовірність k спроб послати як нові, так і раніше не передані кадри за час кадру розподілена за законом Пуассона із середнім числом G спроб. Зрозуміло, що $G \geq S$.

При слабкому завантаженні (S приблизно дорівнює нулю) буде не багато передач, а отже й колізій – G приблизно дорівнює S. При високому

завантаженні $G > S$. При будь–якому навантаженні пропускна здатність це – число кадрів, які треба передати, помножене на ймовірність успішної передачі. Якщо позначити P_0 – імовірність успішної передачі, то відповідно $S = GP_0$.

Розглянемо скільки часу треба відправникові, щоб виявити колізію. Нехай він почав передачу в момент часу t_0 і нехай потрібен час t, щоб кадр досяг самої віддаленої станції. Тоді, якщо в той момент, коли кадр майже досяг цієї віддаленої станції вона почне передачу (адже в системі ALOHA станція спочатку передає, а потім слухає), тобто відправник довідається про це тільки через $t_0 + 2t$.

Імовірність появи *k* кадрів на передачу при розподілі Пуассона дорівнює

$$\Pr[k] = \frac{G^k e^{-G}}{k!}$$

тому ймовірність, що з'явиться 0 кадрів дорівнює e^{-G}. За подвійний час кадру середнє число кадрів буде $2G$, звідси

$$P_0 = e^{-2G},$$

а тому якщо $S = GP_0$, то

$$S = Ge^{-2G}.$$

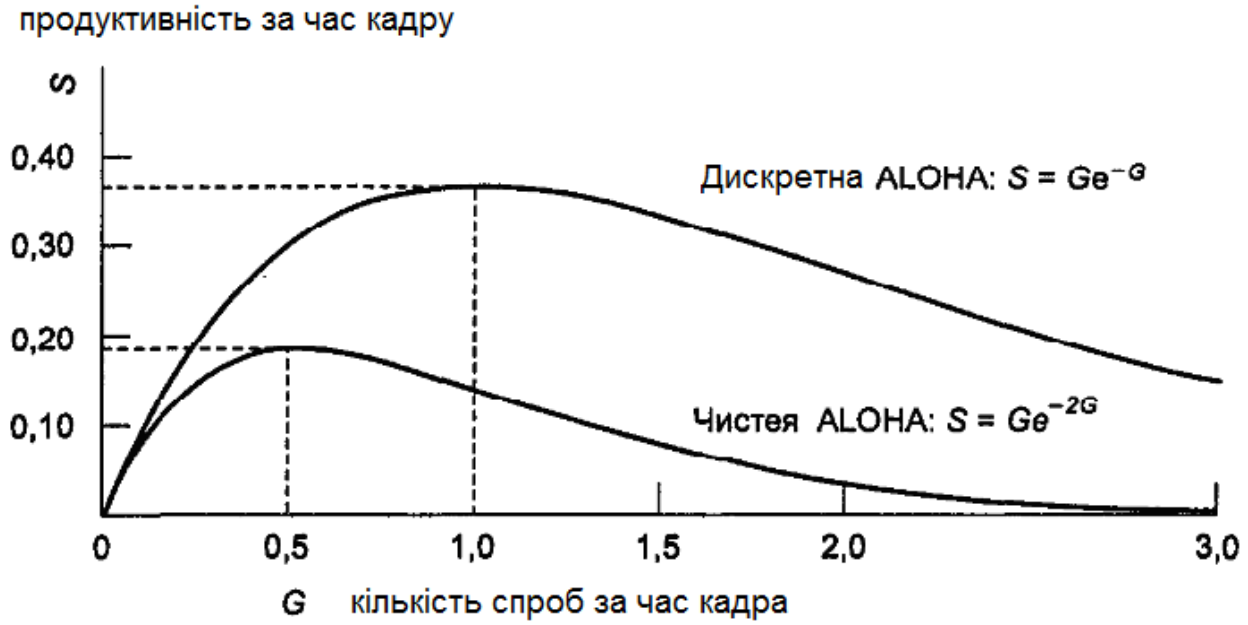


Рисунок 2.7 – Залежність продуктивності каналу від пропонованого трафіка для систем ALOHA

Залежність між навантаженням і пропускною здатністю показана на рис. 2.6. Максимальна пропускна здатність досягається при $G=0.5$ при $S=1/2e$, що становить приблизно 18%. Результат не дуже надихаючий.

2.6.2 Слотована ALOHA.

В 1972 році Робертс запропонував модифікацію чистої ALOHA. Увесь час доступу розділяють на слоти – один кадр на слот. Ясно, що це вимагає синхронізації. Одна станція повинна передавати сигнал на початку чергового слота. Оскільки передачу тепер можна починати не в будь–який момент, а тільки по спеціальному сигналу, то час на виявлення колізії скорочується вдвоє. Звідси

$$S=Ge^{-G}.$$

Як видно з мал. 2.7 максимум пропускної здатності слотованої ALOHA наступає при $G=1$, де $S=1/e$, тобто близько 0,37, що у двоє більше чим у чистої ALOHA.

Розглянемо як G впливає на пропускну здатність підрахуємо ймовірність успішної передачі за k спроб. Тому що e^{-G} ймовірність відсутності колізії при передачі, то ймовірність що кадр буде переданий рівно за k спроб, дорівнює

$$P_k = e^{-G}(1-e^{-g})^{k-1}$$

Середнє очікуване число повторних передач буде

$$E = \sum_{k=1}^{\infty} kP_k = \sum_{k=1}^{\infty} ke^{-G}(1-e^{-G})^{k-1} = e^{G}.$$

Ця експонентна залежність показує, що з ростом G різко зростає число повторних спроб, а отже й падіння загальної пропускної здатності каналу.

2.7 Протоколи множинного доступу з контролем несучої (CSMA).

Протокол множинного доступу до каналу з контролем несучої CSMA (Carrier Sense Multiple Access). Кращий результат, який ми можемо одержати для системи ALOHA – 1/e. Це не дивно, тому що там передаюча станція не звертає увагу на те, що роблять інші. У локальних мережах є можливість визначити, що роблять інші станції й тільки після цього вирішувати що робити.

Протоколи, які реалізують саме цю ідею – визначити чи є передача й діяти відповідно, називаються протоколами з виявленням несучої CSMA (Carrier_Sense_Multiply_Access).

2.7.1 Наполегливі й не наполегливі CSMA.

Відповідно до протоколу, що ми зараз розглянемо, станція перш ніж що–небудь передавати визначає стан каналу. Якщо канал зайнятий, то вона чекає. Як тільки канал звільнився вона намагається почати передачу. Якщо при цьому відбулася колізія, вона очікує випадковий інтервал часу й все починає з початку. Цей протокол називається CSMA наполегливим протоколом першого рівня або 1–наполегливим CSMA протоколом, тому що він починає передачу з імовірністю 1 як тільки виявляє, що канал вільний.

Тут істотною є затримка поширення сигналу. Чим вона більша, тим більше буде колізій, тому що дві готові до передачі станції виявлять що вони обидві в режимі передачі тільки після закінчення часу затримки. Проте цей протокол більш ефективний, чим кожен з ALOHA, тому що враховують що відбувається на каналі перш, ніж почати діяти.

Інший варіант CSMA – не наполегливий CSMA протокол. Основна відмінність його від попереднього в тім, що готова до передачі станція не опитує постійно канал, чекаючи коли він звільнитися, а робить це через випадкові відрізки часу. Це трохи збільшує затримку при передачі, але загальна ефективність зростає.

І , нарешті, CSMA наполегливий протокол рівня p. Він застосовується до слотованих каналів. Коли станція готова до передачі вона опитує канал, якщо він вільний, то вона з імовірністю p передає свій кадр і з імовірністю $q = 1 - p$ чекає наступного слота. Так вона діє поки не передасть кадр. Якщо відбулася колізія вчасної передачі, вона очікує випадковий інтервал часу й опитує канал знову. Якщо при опитуванні каналу він виявився зайнятий, станція чекає початку наступного слота й весь алгоритм повторюється. На рис. 2.8 показано пропускну здатність залежно від навантаження.

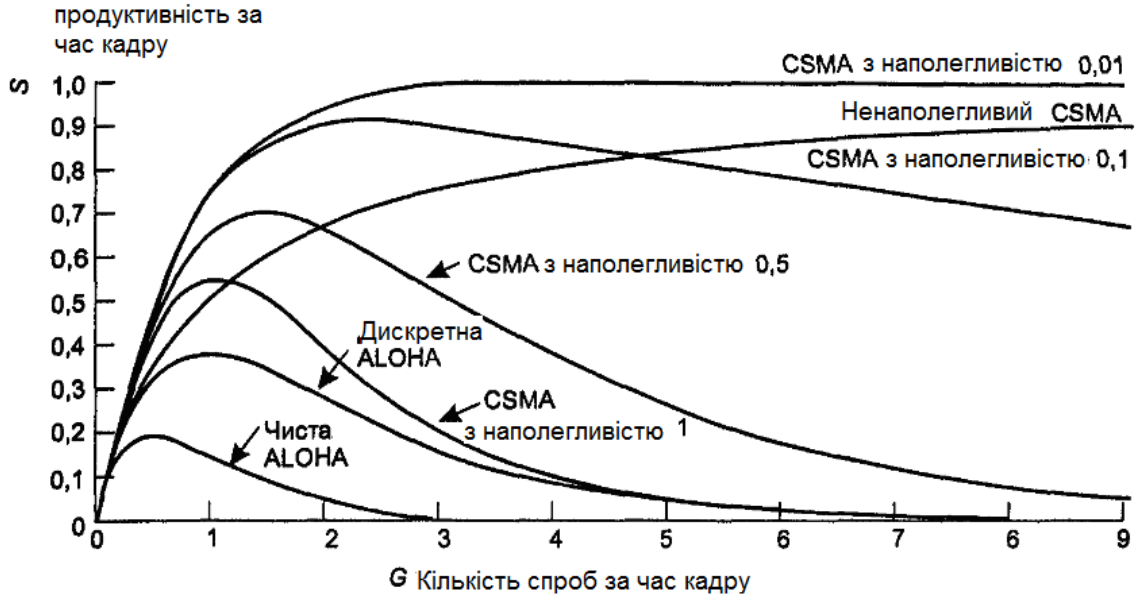


Рисунок 2.8 – Порівняння використання каналу в залежності від його навантаження для різних протоколів колективного доступу

2.7.2 Протоколи конкурентного доступу з контролем несучої з визначенням колізій (CSMA/CD).

Наполегливі й ненаполегливі CSMA протоколи безсумнівно є поліпшення ALOHA, тому що вони починають передачу тільки перевіривши стан каналу. Іншим поліпшенням, яке можна зробити, – станції повинні вміти визначати колізії якомога раніше, а не по закінченні відправлення кадру. Це заощаджує час і пропускну здатність каналу. Такий протокол, відомий як CSMA/CD – «Carrier Sense Multiply Access with Collision Detection» , широко використовується в локальних мережах.

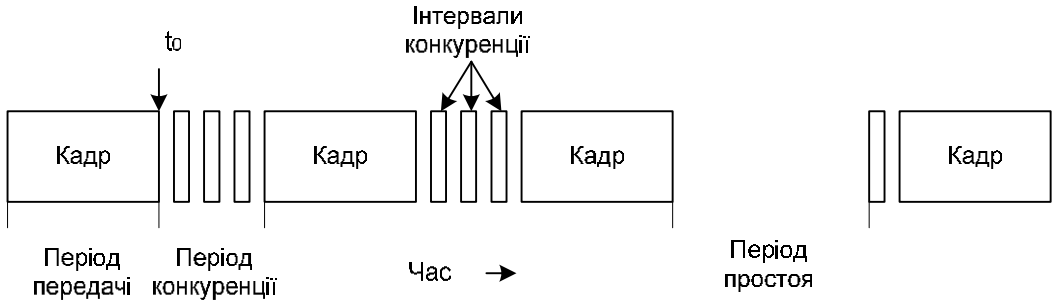


Рисунок 2.9 – Протокол CSMA/CD може перебувати в одному із трьох станів: конкуренції, передачі й простою.

На мал. 2.9 показана модель, що використовується в багатьох протоколах. У момент t0 станція закінчує передачу чергового фрейму. Всі станції, у яких є кадр для передачі починають передачу. Природно відбуваються колізії, що швидко виявляються, порівнюючи відправлений сигнал з тим який є на лінії. Виявивши колізію, станція відразу припиняє передачу на випадковий інтервал часу, після чого все починається спочатку. У такий спосіб у роботі протоколу CSMA/CD можна виділити три періоди: змагань, передачі й очікування, коли немає кадрів для передачі.

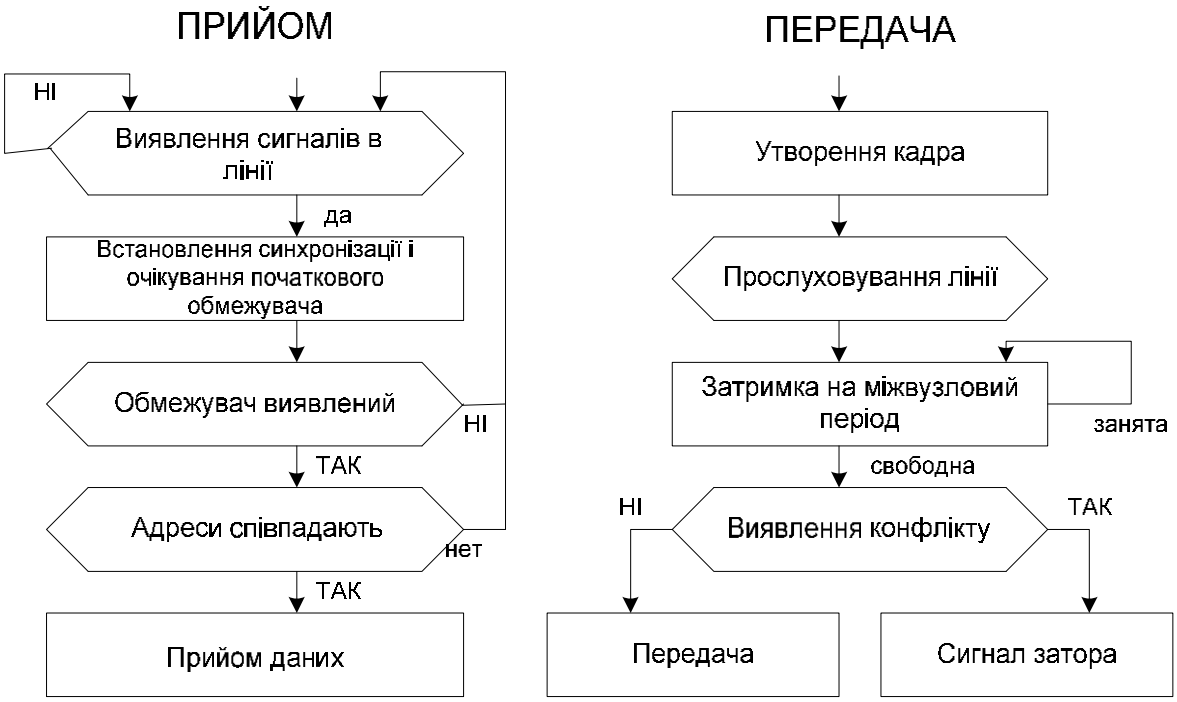


Рисунок 2.10 – Алгоритми прийому й передачі даних у вузлі при CSMA/CD

На рис. 2.10 представлено алгоритми прийому й передачі даних в одному з вузлів при CSMA/CD.

Скільки часу станції, що почала передачу, потрібно, щоб визначити колізію. Позначимо t час поширення сигналу до самої вилученої станції на лінії. Для коаксіалу в 1 км $t = 5\text{ms}$. Тоді мінімальний час для визначення колізії буде $2t$. Тому, станція не може бути впевнена, що вона захопила канал доти, поки в періоді $2t$ секунд не буде колізій. Тому, весь період змагань розбивається на слоти по $2t$ секунд по одному біту на слот. Захопивши канал, станція може далі передавати кадр із будь–якою швидкістю.

Треба підкреслити, що MAC підрівень забезпечує надійну передачу, використовуючи спеціальні прийоми кодування даних. Пізніше, при розгляді Ethernet, ми докладно розглянемо як це досягається.

2.8 Приклади протоколів множинного доступу.

Канальний рівень визначає методи форматування даних для передачі й методи контролю доступу в мережу. У цих розділах розглянуті наступні протоколи канального рівня:

- Ethernet;
- Token Ring;
- FDDI.

FDDI, Token Ring і Ethernet можуть розглядатися як фізичні інтерфейси або логічні протоколи, інкапсульовані в протоколи WAN або ATM.

На рисунку 2.11 показано подання протоколів LAN у моделі OSI.

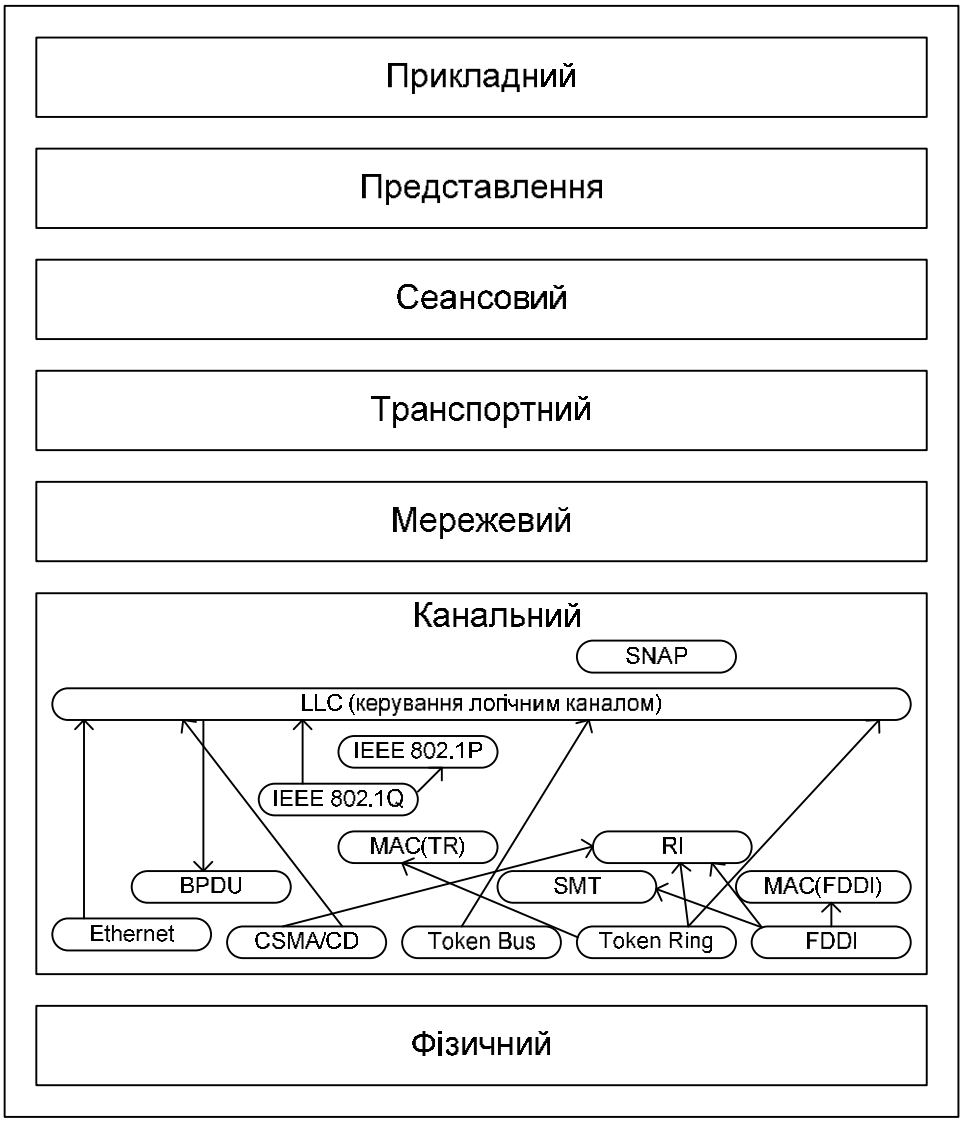


Рисунок 2.11 – Протоколи LAN у моделі ISO/OSI .

2.8.1 Ethernet

Специфікація ANSI/IEEE 802.3 1933–00

Широко використовуваний для побудови комп'ютерних мереж стандарт Ethernet був розроблений компаніями DEL, Intel і Xerox. Ethernet – сама популярна в цей час мережева архітектура. Вона використовує вузькосмугову передачу зі швидкістю від 10 Мбіт/с до 1Гбіт/с, топологію "шина" або "зірка", а для регулювання трафіка у фізичному сегменті – CSMA/CD.

Мережа Ethernet має наступні характеристики:

– специфікації – IEEE 802.3;
– топології – лінійна шина, зірка–шина;
– швидкість передачі даних кабельна система – 10 і 1000 Мбіт/с;
– тип передачі – вузькосмугова;
– метод доступу CSMA/CD;
– кабельна система – товстий і тонкий коаксіальний, UTP.

Структура заголовка Ethernet

Структура заголовка Ethernet показана нарис.2.12.

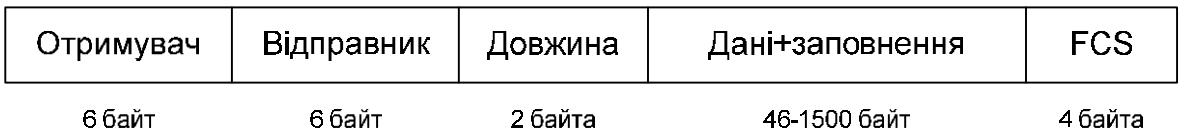


Рисунок 2.12 – Структура заголовка Ethernet

Адреса одержувача

Поле адреси одержувачів має структуру, показану на рис 2.13.

Рисунок 2.13 – Структура адреси одержувачів

I/G Персональний (I) або груповий (G) адреса:

0 персональна адреса DASP;

1 групова адреса DASP.

U/L Універсальний (U) або локальний (L) адреса:

0 універсальна адреса DASP;

1 локальна адреса DASP.

Адреса відправника

Поле адреси відправника має показану на рис.2.14 структуру.

Рисунок 2.14 – Структура адреси відправника

0 Перший біт адреси відправника завжди має нульове значення.

U/L Універсальний(U) або локальний (L) адреса:

0–універсальна адреса SSAP;

1–локальна адреса SSAP.

Довжина / Тип

Для протоколу Ethernet це поле містить ідентифікатор типу Ethernet (використовуваний відправником протокол мережевого рівня – значення, що перевищує 0x0600).

Для 802.3 значення цього поля (46–1500) вказує на довжину поля даних, що є інкапсуляцією протоколу LLC (заголовок LLC казує на тип вкладеного протоколу).

Дані + біти заповнення

Протокол LLC, FSC, Контрольна сума кадру.

2.8.2 Token Ring

Специфікація IEEE 802.3 1995–00

TokenRing є протокол LAN, у якому всі станції з'єднані в (логічне) кільце й кожна станція може приймати дані тільки від свого найближчого сусіда. Дозвіл на передачу визначається спеціальним маркером (TOKEN), переданим по кільцю.

Структура заголовку TokenRing показана на рис. 2.15.

SDEL	1 байт
Керування доступом	1 байт
Керування кадром	1 байт
Адреса отримувача	6 байт
Адреса відправника	6 байт
Відомості про маршрутизацію	0-30 байт
Дані (LLC чи MAC)	Змінна довжина
FCS	4 байта
EDEL	1 байт
Стан кадру	1 байт

Рисунок 2.15 – Структура заголовка TokenRing

SDEL / EDEL .

Початковий (*SDEL*) або кінцевий (*EDEL*) покажчик. Обидва типи полів містять навмисні порушення манчестерського кодування, які дозволяють відрізнити поля SDEL і EDEL у потоці іншої інформації.

Керування доступом

Поле керування доступом має формат, показаний на рис. 2.16.

P	P	P	T	M	R	R	R

Рисунок 2.16 – Структура поля управління доступом

PPP Біти пріоритету: 000 нижчий пріоритет; 111 вищий пріоритет.

T Біт маркера: 0 маркер; 1 кадр.

M лічильник моніторингу: 0 – вихідне значення; 1 – змінено для активного монітора.

R Біти резервування: 000 резервування нижчого пріоритету; 111 – резервування вищого пріоритету.

Керування кадром

Формат поля керування кадром показаний на рис. 2.17:

Тип кадру	0	0	Індикатор

Рисунок 1.17 – Структура поля керування

Поле, що позначає тип кадру приймає наступні значення:

00 MAC – Кадр; 01 – кадр LLC; 10 – тип кадру не визначений; 11 – тип кадру не визначений.

Наступні два біти завжди мають нульові значення. Індикатор показує кадри, для яких адаптер використовує спеціальні засоби буферизації й обробки: 0000 експрес–буфер; 0010 застереження; 0011 маркер претензій; 0100 чищення кільця; 0101 є присутнім активний монітор; 0110 є присутнім неактивний (standby) монітор.

Адреса одержувача

Поле адреси одержувача має структуру, показану на рис 2.18:

I/G	U/L	Біти адреси

Рисунок 2.18 – Структура адреси одержувача

I/G Персональний (I) або груповий (G) адреса:

0 персональна адреса DSAP;

1 групова адреса DSAP.

U/L Універсальний (U) або локальний (L) адреса:

0 універсальна адреса DSAP;

1 локальна адреса DSAP.

Адреса відправника

Поле адреси відправника має загальну структуру рис. 2.19:

Рисунок 2.19 – Структура адреси відправника

RII Індикатор маршрутної інформації:

0 маршрутна інформація відсутня;

1 маршрутна інформація присутня.

I/G Персональний (I) або груповий (G) адреса:

0 персональна адреса SSAP;

1 групова адреса SSAP.

Відомості про маршрутизацію

Поле маршрутної інформації має наступну структуру рис 2.20:

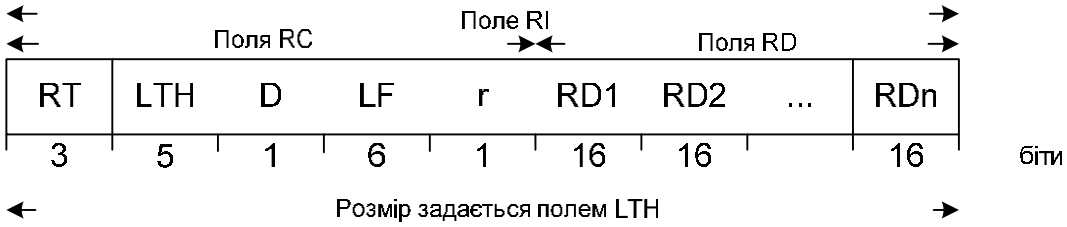


Рисунок 2.20 – Структура поля маршрутної інформації

RC Керування маршрутизацією.

RDn Дескриптор маршруту.

RT Тип маршрутизації.

LTH Довжина

D Біт напрямку.

LF Найбільший кадр.

r Зарезервований.

Дані

Інформаційне поле (дані) може містити дані рівня LLC або MAC. Структура поля показана на рис. 2.21:

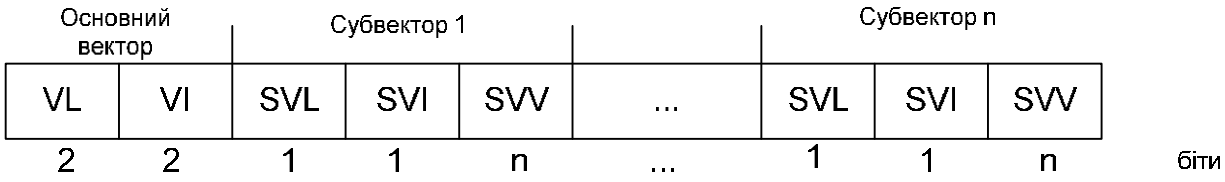


Рисунок 2.21 – Структура інформаційного поля

VL – Довжина основного вектора в октету (байтах).

VI – Ідентифікатор основного вектора.

Поле VI має наступний формат, показаний на рис.2.22.

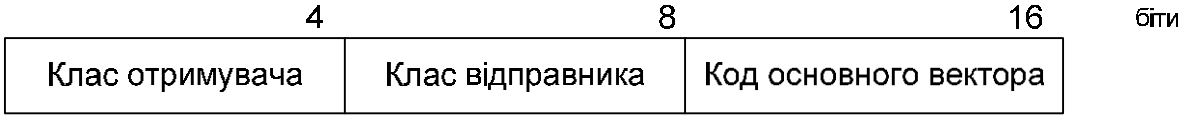


Рисунок 1.22 – Ідентифікатор основного вектора

Клас відправника й одержувача

Поля класу відправника й одержувача забезпечують коректну маршрутизацію в станції кільця:

0 станція кільця;

4 сервер конфігураційних звітів;

5 сервер параметрів кільця;

6 монітор помилок у кільці.

Код основного вектора

Код основного вектора визначає тип цього вектора, наприклад:

0x00 відгук;

0x02 застереження (beacon) і т.д.

SVL – Довжина субвектора в октетах (байтах).

SVI – Код субвектора визначає тип цього вектора, наприклад:

0x00 тип застереження (beacon);

0x02 NAUN (Next Adress. Upstream Neighbor) – адреса сусідньої станції, від якого приходять кадри й т.д.

SVV – Значення субвектора (інформаційне поле змінної довжини).

FCS – Контрольна сума кадру.

Стан кадру

Це поле містить біти, які можуть бути встановлені одержувачем кадру для того, щоб повідомити про розпізнавання адреси й успішне копіювання кадру.

2.8.3 Волоконно-оптичний розподілений інтерфейс передачі даних FDDI

FDDI (Fiber Distributed Data Interface) являє собою технологію передачі даних зі швидкістю 1000 Мбіт/с по подвійному кільцю (з дерев). Стандарт FDDI запропонований Американським інститутом стандартизації (ANSI).

Структура заголовку кадру *FDDI* показана на рис. 2.23.

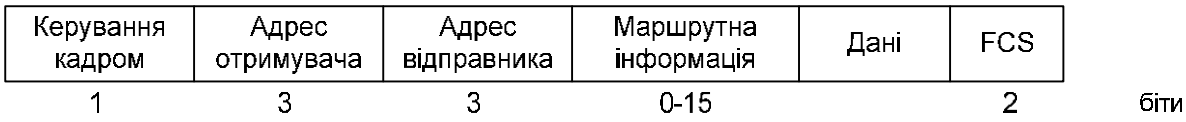


Рисунок 2.23 – Структура заголовка FDDI

Керування кадром.

Поле керування кадром має наступну структуру рис. 2.24:

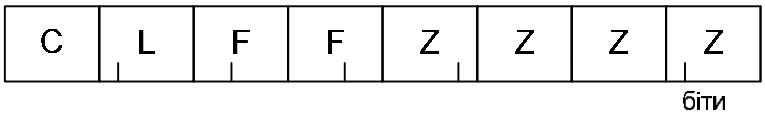


Рисунок 2.24 – Структура поля керування кадром FDDI

C Біт класу:

0 асинхронний кадр;

1 синхронний кадр.

L Біт довжини адреси:

0 16 бітів (не використовується ніколи);

1 48 бітів (використовується завжди).

FF Біти формату.

ZZZZ Біти керування

Адреса одержувача

Поле адреси одержувача має наступну структуру рис 2.25.

Рисунок 2.25 – Структура адреси одержувача

I/G Персональний (I) або груповий (G) адреса:

0 персональна адреса DASP;

1 групова адреса DASP.

U/L Універсальний (U) або локальний (L) адреса:

універсальна адреса DASP;

локальна адреса DASP.

Адреса відправника

Поле адреси відправника має загальну структуру рис. 2.26:

Рисунок 2.26 – Структура адреси відправника

I/G Персональний (I) або груповий (G) адреса:

0 персональна адреса SSAP;

1 групова адреса SSAP.

RII Індикатор маршрутної інформації:

0 маршрутна інформація відсутня;

1 маршрутна інформація присутня.

Маршрутна інформація

Структура поля маршрутної інформації показана на рис. 2.27.

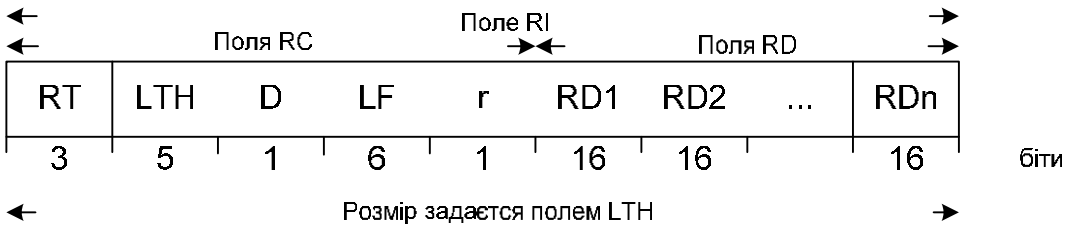


Рисунок 2.27 – Структура поля маршрутної інформації

RC Керування маршрутизацією (16 бітів).

RDn Дескриптор маршруту.

RT Тип маршрутизації.

LTH Довжина

D Біт напрямку.

LF Найбільший кадр.

r Зарезервований.

Дані

Інформаційне поле (дані) може містити протокол MAC, LLC або SMT.

FSC – Контрольна сума кадру.

3 КОНСТРУКТОРСЬКА ПРОЕКТНА ЧАСТИНА

3.1 Архітектура промислових мереж

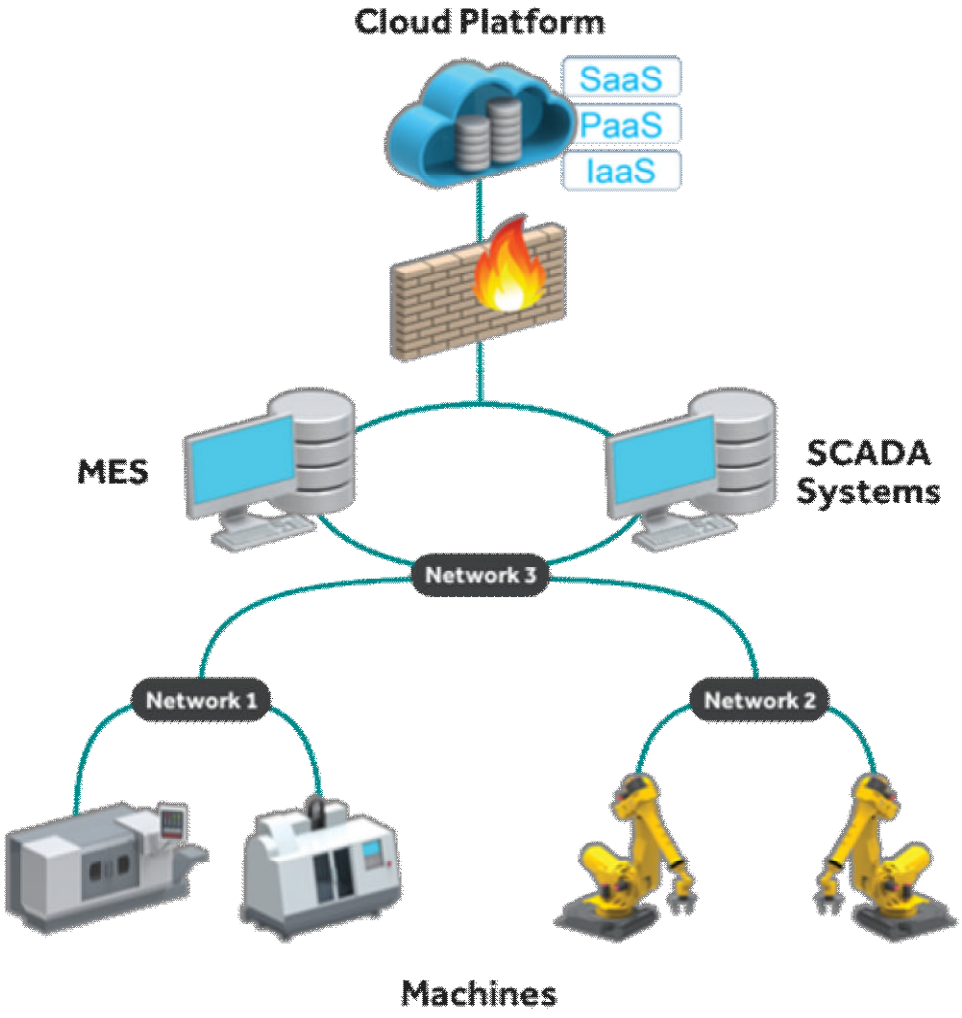


Рисунок 3.1 – Схема архітектури промислових мереж

Промислова мережа є ключовою функцією керування процесом. слід визнати, що ця мережа виходить за межі взаємодії заводських систем, щоб взаємодіяти з системами проектування та документації для формування віртуальної організації та інших пов'язаних систем. Фактичний вибір промислової мережі базується на низці критеріїв, зокрема:

- Детальні вимоги до заявки.
- Можливості мережевих технологій, включаючи вимоги до швидкості та часу.
- Інтеграція з існуючим обладнанням.

- Наявність комплектуючих.
- Витрати на встановлення, обладнання, навчання та обслуговування.

У домені промислових мереж відсутність стандартизації є основною проблемою зв’язку між комп’ютерами. Велика кількість характеристик і топологій сигналу є лише частиною проблеми.

Обмін даними в мережі може бути як асинхронним, так і синхронним, залежно від використовуваного протоколу.

Асинхронний зв'язок:

У асинхронних комунікаціях кожне слово даних надсилається як окреме повідомлення. Асинхронний зв'язок зазвичай достатній, якщо один з одним підключено лише два комп'ютери.

Онлайн-програмування та моніторинг часто виконуються асинхронно за допомогою одного комп’ютера, безпосередньо підключеного до ПЛК, робота чи інших контролерів.

Синхронний зв'язок:

Повідомлення даних синхронного зв’язку складаються з багатьох слів даних, яким передує заголовок, що містить інформацію про «пакет» даних, а за ним іде нижній колонтитул, що містить інформацію перевірки помилок. Синхронний зв’язок доречний, коли потрібно швидко передати великі обсяги даних.

Локальні мережі (LAN) використовують синхронну передачу даних.

Промислові мережі:

Ієрархія промислової мережі, починаючи від корпоративної мережі для корпоративної інформації до взаємозв’язку окремих датчиків через шину датчиків.

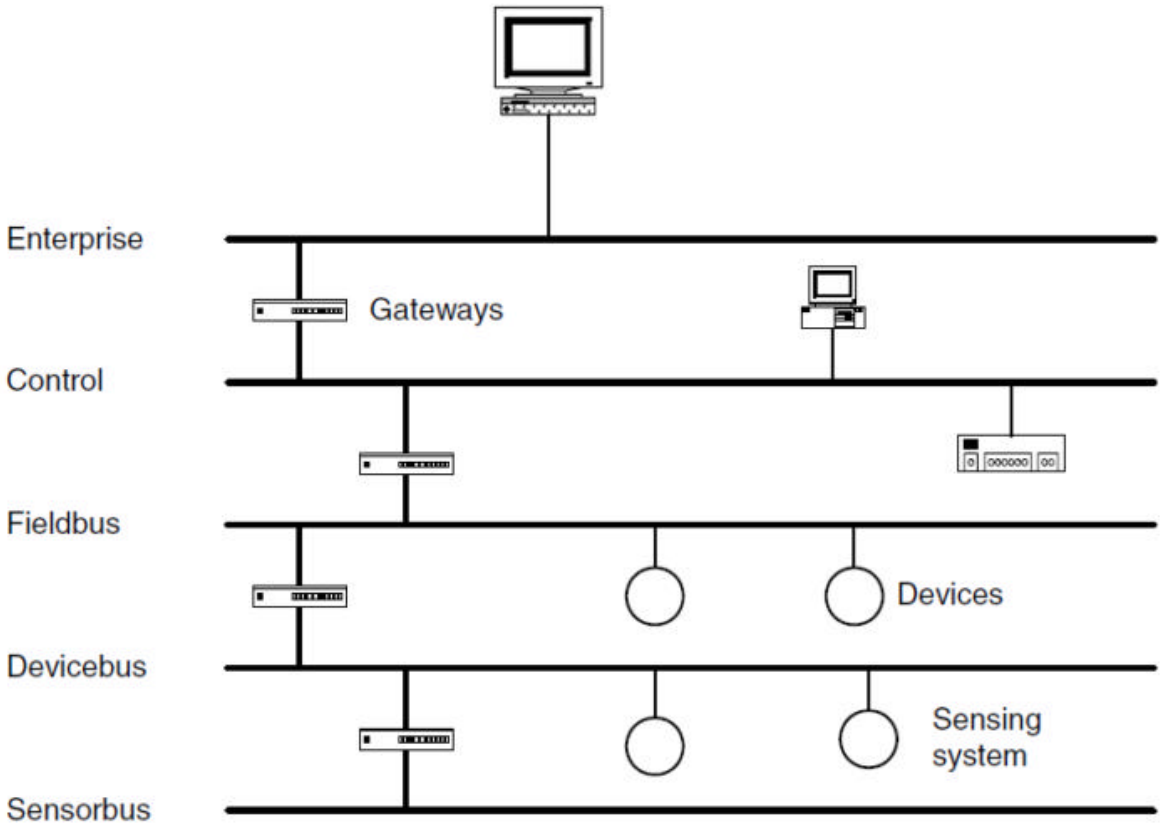


Рисунок 3.2 – Схема промислової мережі по рівнях

На рівні датчика/виконавчого механізм сигнали бінарних датчиків і виконавчих механізмів передаються через шину датчик/виконавчий механізм. На цьому рівні важливою вимогою є недорога техніка, за допомогою якої дані та джерело живлення 24 вольта для кінцевих пристроїв передаються за допомогою загального середовища. Дані передаються суто циклічно.

На польовому рівні розподілені периферійні пристрої, включаючи модулі вводу/виводу, вимірювальні перетворювачі, приводи, клапани та операторські термінали, потребують зв’язку з системами автоматизації через системи зв’язку в реальному часі.

На рівні автоматизованої комірки програмовані контролери, такі як PLC і IPC, спілкуються один з одним. Інформаційний потік вимагає великих пакетів даних і великої кількості потужних комунікаційних функцій. Плавна інтеграція в загальнокорпоративні системи зв’язку, такі як інтранет та Інтернет через TCP/IP та Ethernet, зараз стає важливою вимогою.

Щоб показати ключові функції на кожному рівні ієрархії, нижче наведено огляд ряду систем.

3.2 Стандарти в промислових мережах

3.2.1 Ethernet.

Ethernet вважається найпоширенішою технологією локальної мережі (LAN), і як така використовується в більшості промислових організацій, але зазвичай обмежується офісним середовищем. Протокол Ethernet офіційно вказано в стандарті IEEE 802.3.

Локальна мережа Ethernet зазвичай використовує коаксіальний кабель або спеціальні види крученої пари як середовище передачі. Однією з ключових особливостей системи є відсутність живлення по шині, тому всі концентратори та периферійні пристрої потребують незалежного живлення.

3.2.2 DeviceNet

DeviceNet (DeviceNet, 2005) — це цифрова багатоточкова мережа, яка здатна працювати між промисловими контролерами та пристроями введення/виведення та вважається фактичним стандартом у напівпровідниковій промисловості США.

В архітектурі DeviceNet кожен пристрій і/або контролер вважаються вузлом мережі. Однією з важливих особливостей цієї технології є те, що живлення здійснюється по мережі. Це дозволяє живити пристрої з обмеженими вимогами до потужності безпосередньо від мережі, зменшуючи точки підключення, фізичні розміри та вартість. DeviceNet відповідає моделі OSI і як такий є відкритим стандартом.

DeviceNet – протокол для промислової мережі CAN . Використовується для зв'язку датчиків , виконавчих пристроїв та програмованих логічних контролерів між собою. Відкритий стандарт . Широко застосовується на

транспорті, у машинобудуванні та промисловості. Досить широко поширений у Росії.

DeviceNet — протокол верхнього рівня, розроблений 1994 року компанією Rockwell Automation . Служить для об'єднання в єдину систему пристроїв промислової автоматики, таких як фотодатчики , термодатчики, зчитувачі штрих-кодів , елементи ЧМІ (людино-машинного інтерфейсу), з пристроями, що управляють (комп'ютерами, ПЛК). Мережа має шинну топологію. Допускає «гаряче» підключення та відключення модулів.

Функціональне виконання

Стандарт на промислову мережу DeviceNet, крім протоколу, описує:

відкриті та герметизовані типи роз'ємів пристроїв

діагностичні індикатори (світлодіоди)

профайли (файли параметрів) пристроїв

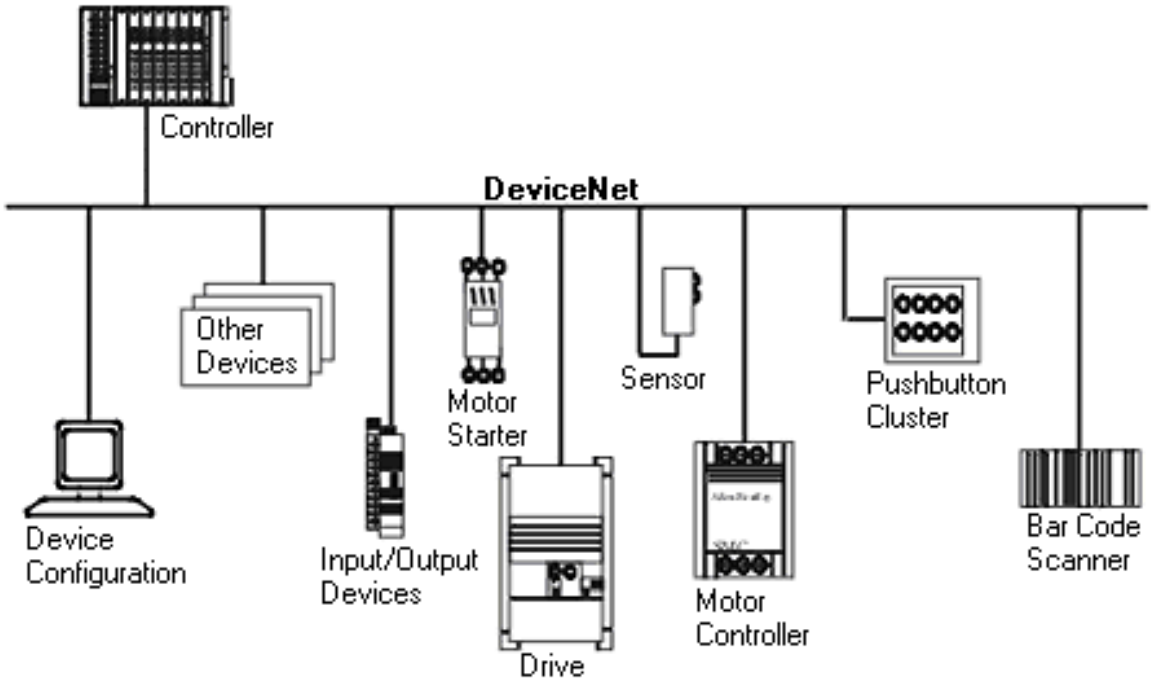


Рисунок 3.3 – Схема мережа DeviceNet

Мережа DeviceNet підтримує:

- читання стану увімк./вимк. датчиків
- керування пусковими пристроями
- передачу температури та струму навантаження пускового пристрою

- зміна швидкості уповільнення приводів
- регулювання чутливості датчиків
- і так далі.

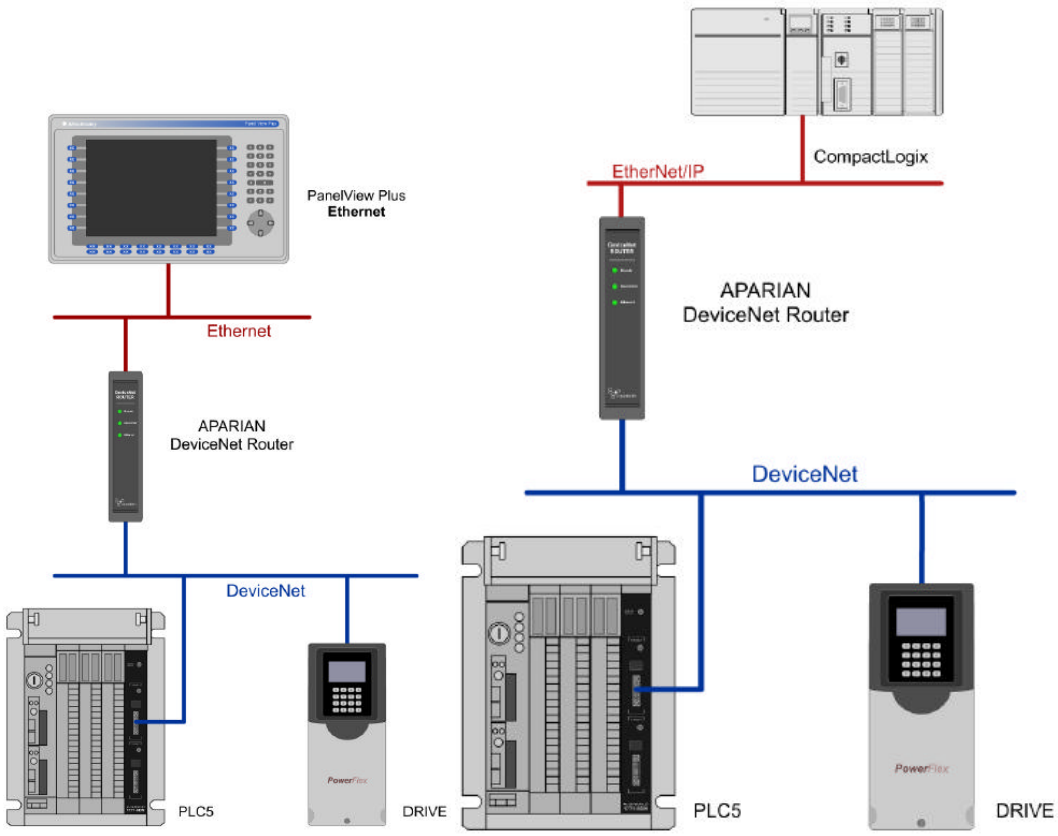


Рисунок 3.4 – Приклади реалізації мережі DeviceNet

Пристрої можуть бути видалені та замінені без відключення інших пристроїв та без інструментів програмування, що допомагає знизити експлуатаційні витрати.

Мережева установка пристроїв економічно вигідніша, ніж традиційна комутація входів/виходів у багатьох додатках, особливо коли пристрої віддалені один від одного на відстань у десятки та сотні метрів.

Зв'язок між різними мережами

Повідомлення від вузла, що знаходиться в мережі ControlNet , DH+ або Промисловий Ethernet , можуть перенаправлятися шлюзом ControlLogix до вузла мережі DeviceNet.

Взаємозамінність. Прості пристрої численних постачальників (наприклад, кнопки, пускові пристрої, фотоелементи, кінцеві вимикачі тощо), які відповідають стандарту мережі DeviceNet і стандарту профайлів пристроїв, взаємозамінні, ніж забезпечують користувачеві гнучкість і можливість вибору.

Одна загальна мережа . Відкритий стандарт мережевих пристроїв забезпечує загальні рішення для кінцевого користувача, зменшуючи постачальників необхідність підтримувати на ринку різні мережі.

Зменшення простоїв . Діагностика забезпечує попереджувальні повідомлення про відмови та полегшує пошук несправностей. Мережа DeviceNet призначена для додатків, які потребують:

- зменшення кількості провідних з'єднань
- швидкої установки та запуску
- гнучкості у можливості додавання або переміщення пристроїв та сегментів кабелів
- малого часу відгуку
- діагностики пристроїв, критичних до простоїв

Конструкція елементів мережі DeviceNet.

Як приєднувачі використовуються штирьові роз'єми, сторона, що приймає, — «мама», що подає сигнал «тато», а також приєднувачі типу, що проколює ізоляцію (такі приєднувачі і кабелі відповідно складаються всього з чотирьох проводів — виключений екран).

Для підключення модулів використовується прямокутний малогабаритний роз'єм п'ятиконтактний Phoenix Contacts з однорядним виконанням. Є два різновиди роз'єму - для підключення одного та двох комплектів кабелів.

Для з'єднання кабелів, що утворюють магістралі, а також для відводів, використовуються різні кабелі - крім п'ятипровідних, що реалізує стандартне підключення до шини, існують дев'ятипровідні кабелі в яких є додаткове живлення, понад існуючі ланцюги: одна пара забезпечує підведення постійної

напруги 24 вольта з джерела живлення обмежується лімітом 3,8 ампер (служить для запитки модулів, пристроїв та/або виконавчих механізмів в мережі), ще одна пара забезпечує підведення змінної напруги 120 вольта (служить для запиту джерел вторинного електроживлення ланцюгів).

Архітектура DeviceNet.

Фізичний рівень.

DeviceNet підтримує швидкості 125, 250 та 500 кбіт/с. Швидкість залежить від довжини кабелю та його типу максимально до 500 м. Типова довжина кабелю – 100 м. Для кабелю завдовжки 380 м швидкість буде 125 кбіт/с, для 75 м – 500 кбіт/с.

Рівень передачі

Формат кадру передачі даних мережі CAN

1 Bit => Start of Frame

11 Bits => Identifier

1 Bit => RTR Bit

6 Bits => Control Field

0-8 Bytes => Data Field

15 Bits => CRC Sequence

1 Bit => CRC Delimiter

1 Bit => Acknowledge

1 Bit => Ack Delimiter

7 Bits => End of Frame

>2 Bits => Interframe Space

3.2.3 PROFIBUS.

PROFIBUS (PROFIBUS, 2005) або Process Field Bus базується на стандарті IEC 61158 і в основному використовується на польовому рівні з можливостями роботи аж до датчиків або аж до виробничих рівнів.

Ряд варіантів розроблено для роботи на заводі (PROFIBUS DP), керування рухом (PROFIdrive), технологічного процесу (PROFIBUS PA) або програм безпеки (PROFIsafe). У PROFIBUS DP і PROFIdrive зв’язок базується на RS485 і має швидкість до 31,25 Кбіт/с на відстані до 1900 м, а також використовує логічне кільце маркерів із парадигмою головний/підлеглий.

3.2.4 Стандарт WirelessHART

Основи мережевого протоколу wireless HART

Стандарт WirelessHART™ забезпечує надійний бездротовий протокол для повного спектру програм вимірювання процесів, контролю та управління активами. Він додає бездротові можливості до протоколу HART , зберігаючи при цьому сумісність з існуючими пристроями, командами та інструментами HART.

Пристрій WirelessHART використовує номінальну частоту передачі 2,4 ГГц за допомогою радіостанцій стандарту IEEE 802.15.4, оскільки відповідність цим критеріям дозволяє пристрою WirelessHART не ліцензувати відповідно до стандартів FCC (Федеральної комісії зі зв’язку).

Бездротова мережа HART:

WirelessHART – це підмножина стандарту зв’язку промислових приладів HART від версії 7, яка передає дані процесу через радіохвилі 2,4 ГГц. WirelessHART – це протокол бездротової сітчастої мережі для програм автоматизації процесів.

Кожен окремий прилад у бездротовому з’єднанні HART підключається через сітчасту мережу. Кожен окремий прилад підключається до загального вхідного та настроювального приладів. Якщо прилад знаходиться далеко від шлюзу або маршрут заблоковано, він не може підключитися до шлюзу. Хоча ви можете спілкуватися зі шлюзом через інші інструменти. Тому кожен пристрій у сітчастій мережі може служити маршрутизатором для повідомлень від інших пристроїв.

Метою сітчастої мережі є забезпечення надлишкових шляхів передачі даних у разі збою пристрою або змін у середовищі, які переривають радіозв'язок між пристроями.

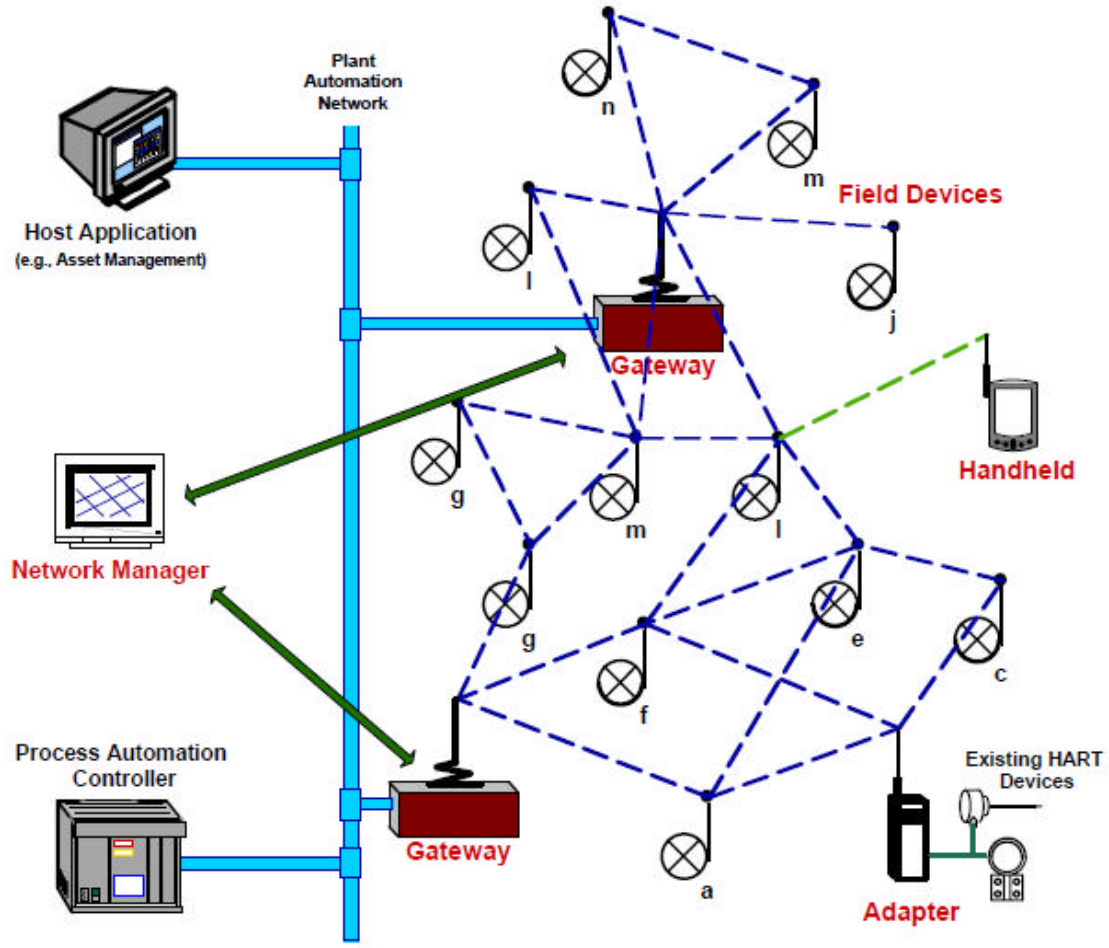


Рисунок 3.5 – Приклади реалізації мережі WirelessHART.

Адміністратор мережі, відповідальний за налаштування мережі, планування зв'язку між пристроями, керування маршрутами повідомлень і моніторинг стану мережі. Network Manager можна інтегрувати в шлюз, головну програму або контролер автоматизації процесу.

Це розширює охоплення мережі та забезпечує резервні шляхи зв'язку для підвищення надійності. Менеджер мережі визначає надлишкові маршрути на основі затримки, ефективності та надійності. Щоб резервні маршрути залишалися відкритими та безперешкодними.

Протокол WirelessHART:

Фізичний рівень:

- Діапазон сигналу від 2,4 ГГц до 2,5 ГГц («ISM» – промисловий, науковий, медичний)
- Модуляція O-QPSK (зміщена квадратурна фазова маніпуляція)
- Швидкість передачі даних 250 кбіт/с
- Розширення спектру прямої послідовності (DSSS) зі стрибкоподібним перемиканням частоти між 15 каналами в межах цього діапазону для безпеки та зменшення перешкод
- Арбітраж шини TDMA (множинний доступ із розподілом часу) з часовими інтервалами 10 мілісекунд, виділеними для передачі пристрою
- Змінна потужність передачі, за замовчуванням 10 дБм (10 міліват).

Рівень каналу даних:

- Ідентифікаційний номер мережі унікально ідентифікує кожну мережу WirelessHART, дозволяючи кільком мережам перекривати одну фізичну область
- «Чорний список» каналів – автоматично запобігає переходу на галасливі канали

Мережевий рівень:

- «Mesh» мережа
- Повторення сигналу – пристрої можуть діяти як «повторювачі» для інших пристроїв, розташованих занадто далеко від головного пристрою
- Пристрій Network Manager визначає маршрути зв’язку між польовими пристроями, а також розклади часу
- Чотири рівні пріоритету повідомлень даних (у списку від найвищого до найнижчого): команда, дані обробки, нормальний (усі повідомлення, окрім команди), тривога.

Прикладний рівень:

- 128-бітне шифрування даних

- Зворотна сумісність із дротовою структурою команд HART і DDL (мова опису пристрою)

3.2.5 Стандарт FOUNDATION Fieldbus.

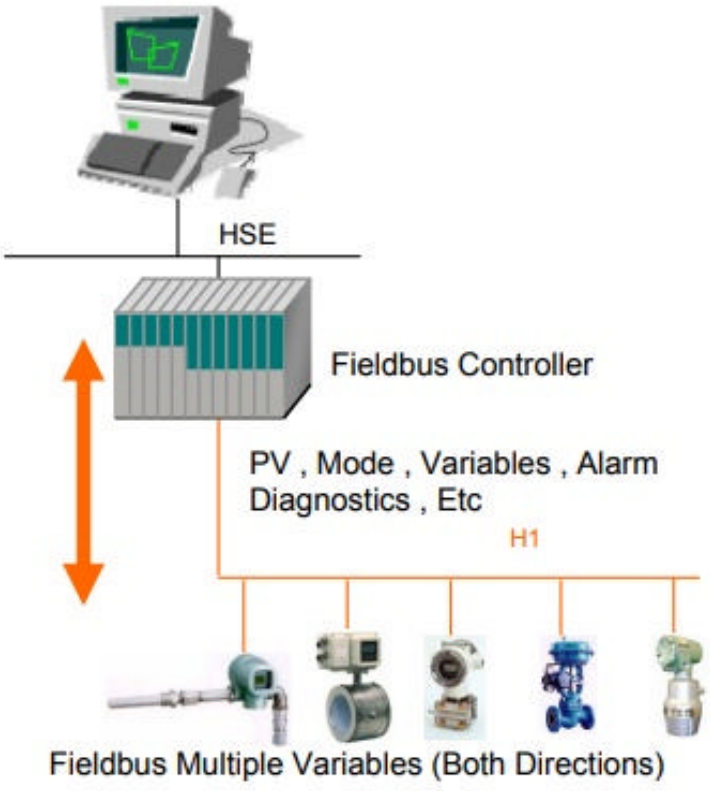


Рисунок 3.6 – Приклад реалізації мережі FOUNDATION Fieldbus

FOUNDATION Fieldbus — це стандарт для цифрових польових приладів, що дає змогу польовим приладам не лише спілкуватися один з одним у цифровому вигляді, а й виконувати всі алгоритми безперервного керування (такі як PID, регулювання співвідношення , каскадне керування , керування з упередженим зв’язком тощо), традиційно реалізоване у спеціальних пристроях керування.

По суті, FOUNDATION Fieldbus розширює загальну концепцію розподіленої системи керування (DCS) аж до самих польових пристроїв. Таким чином, FOUNDATION Fieldbus виділяє себе як більше, ніж просто ще одну

«шину» цифрового зв’язку для промисловості – вона справді представляє новий спосіб реалізації систем вимірювання та керування.

Цей стандарт промислової мережі вперше було запропоновано як концепцію в 1984 році та офіційно стандартизовано Fieldbus Foundation (організація, яка контролює всі стандарти FF і валідацію) у 1996 році. На сьогоднішній день впровадження FF відбувається дещо повільно, здебільшого обмежуючись проектами нового будівництва. . Однією з переваг FF є скорочення часу встановлення, що робить цю технологію більш привабливою для абсолютно нових установок, ніж для проектів модернізації.

Щоб зрозуміти, наскільки FF відрізняється від інших систем цифрових приладів, розглянемо типову схему розподіленої системи керування (DCS), де всі обчислення та логічні «рішення» приймаються спеціальними контролерами, які зазвичай мають форму мультикарти. «стійка» з процесором(ами), платами аналогового введення, платами аналогового виведення та іншими типами плат вводу/виводу (вводу/виводу):

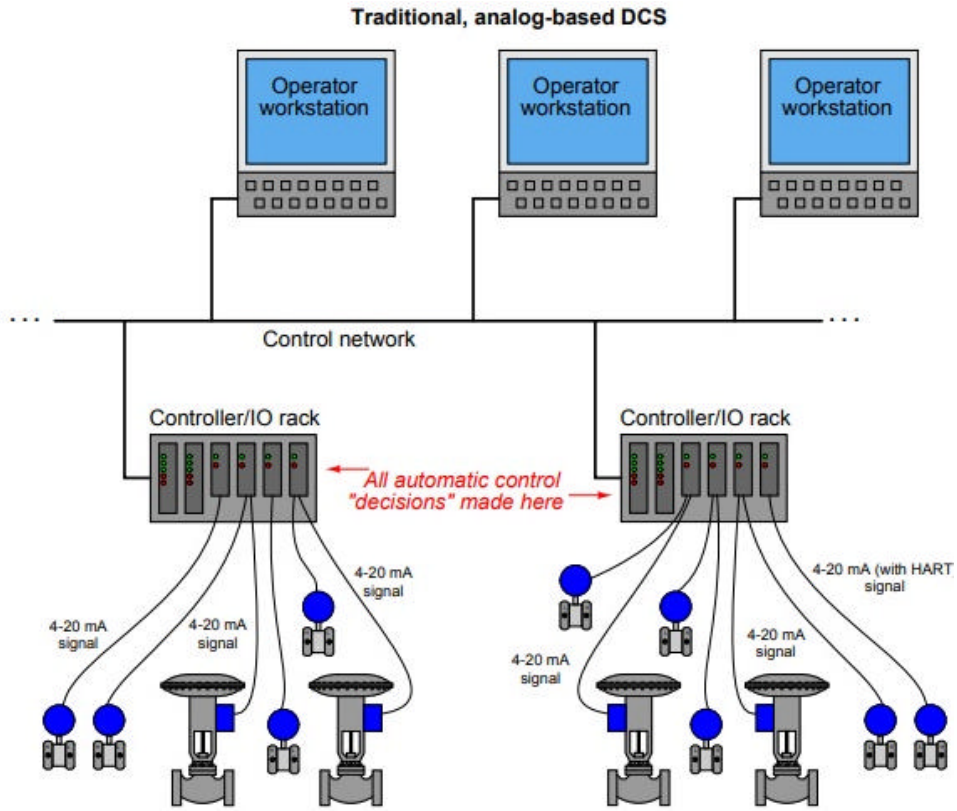


Рисунок 3.7 – Приклад реалізації мережі FOUNDATION Fieldbus

Інформація передається в аналоговій формі між контролерами DCS і польовими приладами. За наявності відповідних типів плат вводу/виводу DCS може навіть обмінюватися цифровими даними з деякими польовими приладами за допомогою протоколу HART. Це дозволяє багатопараметричним приладам передавати кілька змінних до та з контролерів DCS (хоча й повільно) через одну пару проводів

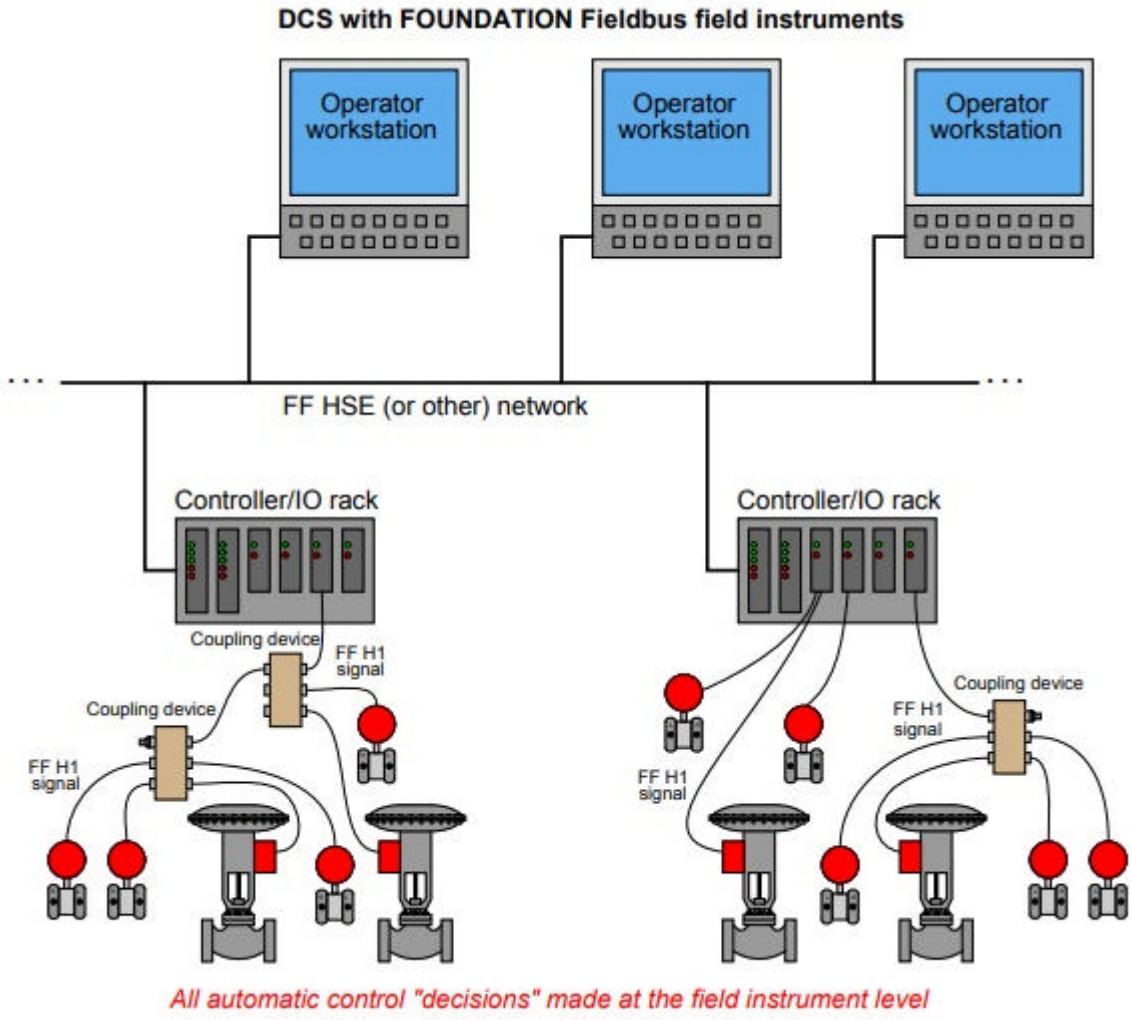


Рисунок 3.8 – Приклад реалізації мережі FOUNDATION Fieldbus з контролерами DCS.

Коли розроблявся стандарт FF, було заплановано два різних рівня мережі: «низькошвидкісна» мережа для підключення польових приладів один до одного для формування мережевих сегментів і «високошвидкісна» мережа для використання в якості загальнозаводської « магістраль» для передачі великих обсягів даних процесу на великі відстані.

Низькошвидкісна (польова) мережа була позначена H1, а високошвидкісна (заводська) мережа була позначена H2. Пізніше в процесі розробки стандарту FF було зрозуміло, що існуюча технологія Ethernet задовольнить усі основні вимоги високошвидкісної «магістралі», тому було вирішено відмовитися від роботи над стандартом H2, зупинившись на розширенні до 100 Мбіт/с. Ethernet під назвою HSE («Високошвидкісний Ethernet») замість цього є магістральною мережею FF.

Мінімальний сегмент FF H1 складається з джерела живлення постійного струму, «кондиціонера живлення», рівно двох кінцевих резисторів1 (по одному на кожному крайньому кінці кабелю), екранованого кабелю з витою парою та, звичайно, щонайменше двох інструментів FF для спілкуватися один з одним. Кабель, що з'єднує кожен прилад із найближчим роз'єднанням, називається відгалуженням (або інколи шлейфом або роз'єднанням), тоді як кабель, що з'єднує всі роз'єднання з основним джерелом живлення (де зазвичай розташовується хост DCS), називається магістральним (або іноді домашній запуск для розділу, що веде безпосередньо до хост-системи):

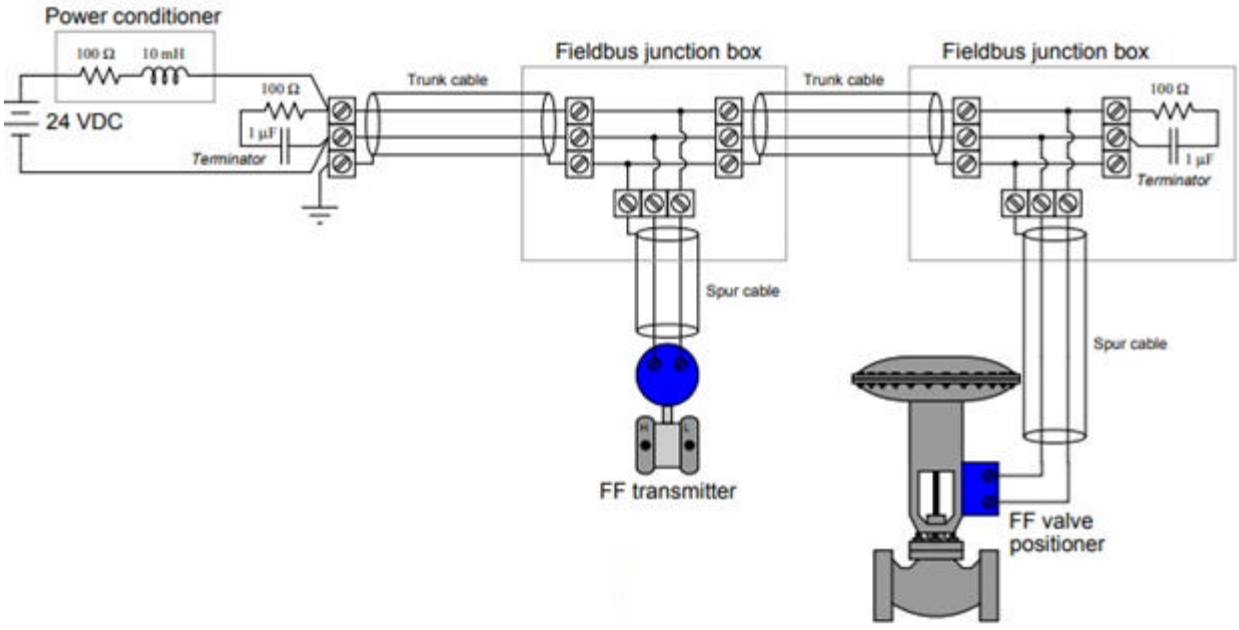


Рисунок 3.7 – Приклад реалізації зв'зків мережі FOUNDATION Fieldbus

3.3 Розробка архітектури промислової автоматизації

У цьому розділі представлені основні концепції та міркування щодо середовищ промислової автоматизації.

Логічна структура заводу

У 20 столітті відбулося значне зростання виробництва промислових процесів і вертикалей, від комунальних послуг до процесів і дискретного виробництва. Ці розробки були значною мірою викликані прогресом автоматизації та технологій керування, включаючи винахід програмованих логічних контролерів (ПЛК), промислових роботів, машин з комп'ютеризованим числовим керуванням (верстатів) тощо; вони в парі з програмними додатками, такими як SCADA, Manufacturing Execution System (MES) і системами Historian і Asset Management, запустили IACS.

Щоб зрозуміти вимоги безпеки та мережевих систем IACS, у цьому посібнику використовується логічна структура для опису основних функцій і складу промислової системи. Модель Пердью для ієрархії управління (довідковий номер ISBN 1-55617-265-6) є поширеною та добре зрозумілою моделлю в галузі, яка сегментує пристрої та обладнання за ієрархічними функціями. Ґрунтуючись на цій сегментації технології IACS, Комітет Міжнародного товариства автоматизації ISA-99 з безпеки промислових систем і систем керування та структура промислової кібербезпеки IEC 62443 визначили рівні та логічну структуру, показані на рисунку 3.

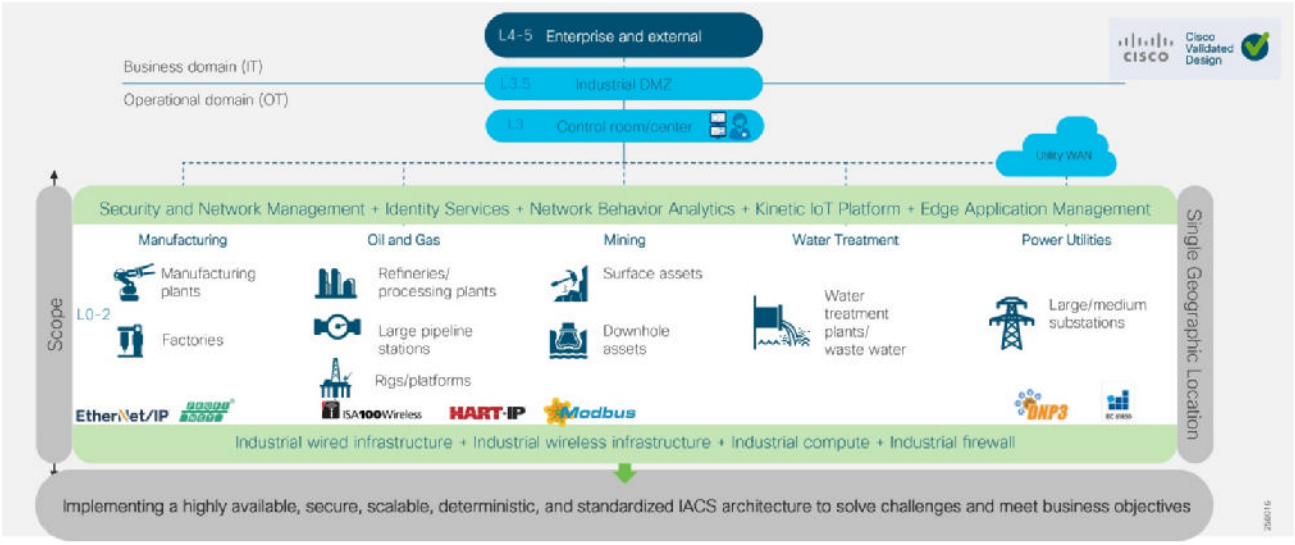


Рисунок 3.8 – Приклад реалізації еталонної архітектури промислової автоматизації.

3.3.1 Функції рішення Cisco Industrial Automation

Це рішення для промислової автоматизації застосовує найкращі IT-можливості та досвід, налаштовані та узгоджені з вимогами та додатками OT, і забезпечує для промислових середовищ:

- Висока доступність для всіх ключових промислових комунікацій і послуг
- Підтримка детермінованих програм у режимі реального часу з низькою затримкою мережі та тремтінням для найскладніших програм, таких як керування рухом
- Можливість розгортання в різних промислових умовах за допомогою IT-обладнання промислового та комерційного виробництва (COTS).
- Можливість масштабування від невеликих (десятки до сотень пристроїв IACS) до дуже великих (від тисяч до 10 000) розгортань
- Керованість на основі намірів і простота використання для полегшення розгортання та обслуговування, особливо персоналом OT з обмеженими IT-можливостями та знаннями
- Сумісність із промисловими постачальниками, зокрема Rockwell Automation, Schneider Electric, Siemens, Mitsubishi Electric, Emerson, Honeywell, Omron і SEL

- Покладення на відкриті стандарти для забезпечення вибору постачальника та захисту від обмежень власності
- Розподіл точного часу на сайті для підтримки додатків руху та збору даних розкладу подій
- Конвергентна мережа для підтримки зв’язку від датчика до хмари, що дає змогу використовувати багато випадків промисловості 4.0
- IT-архітектура безпеки, яка інтегрує контекст OT, застосовна та підтверджена для промислових додатків (досягає найкращих практик як для OT, так і для IT-середовищ)
- Розгорніть додаток IoT із підтримкою Edge Compute
- Орієнтований на OT безперервний моніторинг кібербезпеки пристроїв і комунікацій IACS

Щоб зрозуміти вимоги безпеки та мережевих систем IACS, використовується логічна структура для опису основних функцій і складу промислової системи. Модель Пердью для ієрархії управління (довідковий номер ISBN 1-55617-265-6) є поширеною та добре зрозумілою моделлю в галузі, яка сегментує пристрої та обладнання за ієрархічними функціями. Ґрунтуючись на цій сегментації технології IACS, Комітет Міжнародного товариства автоматизації ISA-99 з безпеки промислових систем і систем керування та структура промислової кібербезпеки IEC 62443 визначили рівні та логічну структуру, показані на рисунку 3.9

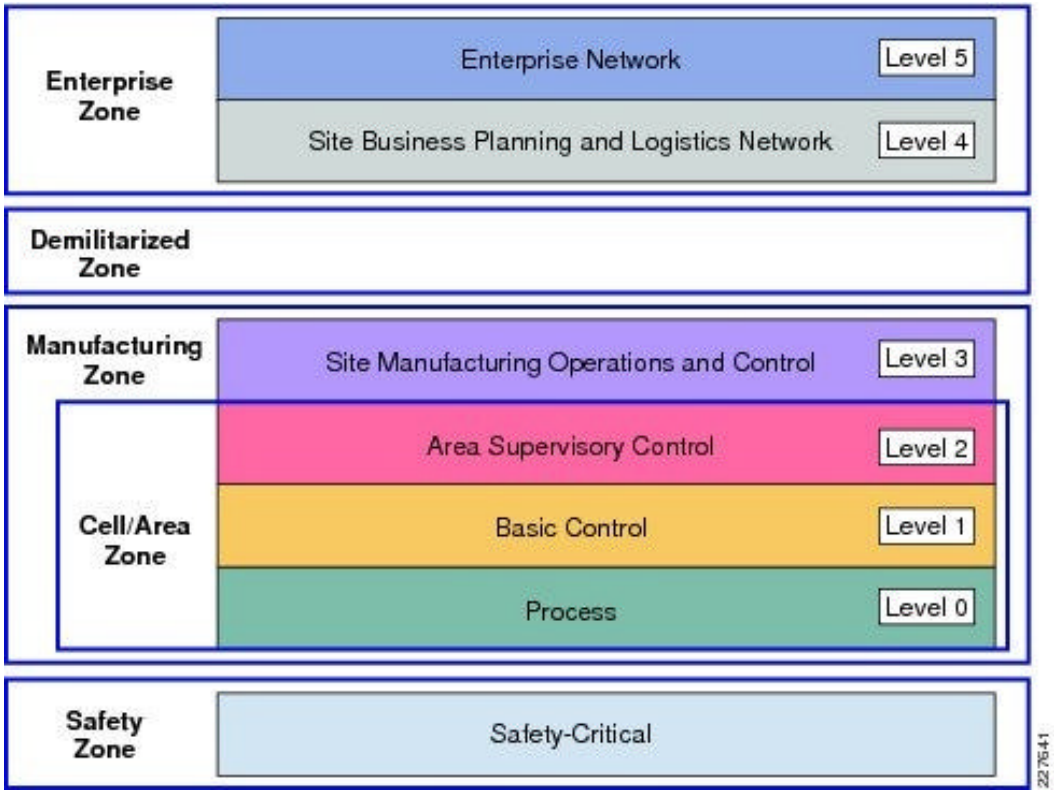


Рисунок 3.9 – Приклад реалізації логічної, еталонної архітектури структури заводу.

Таблиця 3.1 – Переваги та недоліки топології мережі IACS для мережі доступу.

Тип	Переваги	Недоліки
Ндлишкова зірка	Стійкість до багатьох збоїв підключення. Швидша конвергенція до втрати з'єднання Постійна кількість переходів (зазвичай два в плоскому дизайні) забезпечує передбачувану та стабільну продуктивність і характеристики в реальному часі Менша кількість вузьких місць у дизайні зменшує ймовірність надмірної підписки на сегмент	Додаткова проводка (і відповідні витрати), необхідна для підключення комутаторів доступу рівня 2 безпосередньо до комутатора розподілу рівня 3Додаткова складність конфігурації (наприклад, Spanning Tree з кількома блоками)
кільце	Стійкість до втрати одного мережевого підключення Менша складність кабельної розводки в деяких плануваннях цеху Кілька шляхів зменшує ймовірність надмірної підписки та вузьких місць	Додаткова складність конфігурації (наприклад, Spanning Tree з одним блоком)Довший час конвергенції Змінна кількість переходів ускладнює проектування передбачуваної продуктивності
Лінійна/зіркова	Легко розробити, налаштувати та реалізуватиНайменша кількість кабелів (і відповідні витрати)	Втрата мережевої служби у разі збою з'єднання (немає стійкості)Створює вузькі місця на з'єднаннях, найближчих до пристрою рівня 3, а змінна кількість переходів ускладнює забезпечення надійної роботи.

Конвергенція моделі підприємства з додатками IACS і моделлю Purdue, ми маємо еталонну архітектуру високого рівня на малюнку 3.10. Ця схема відображає основні рівні, рівні розподілу та доступу, операції та контроль сайту, а також зону комірки/зони. Це лише еталонна архітектура дротової мережі.

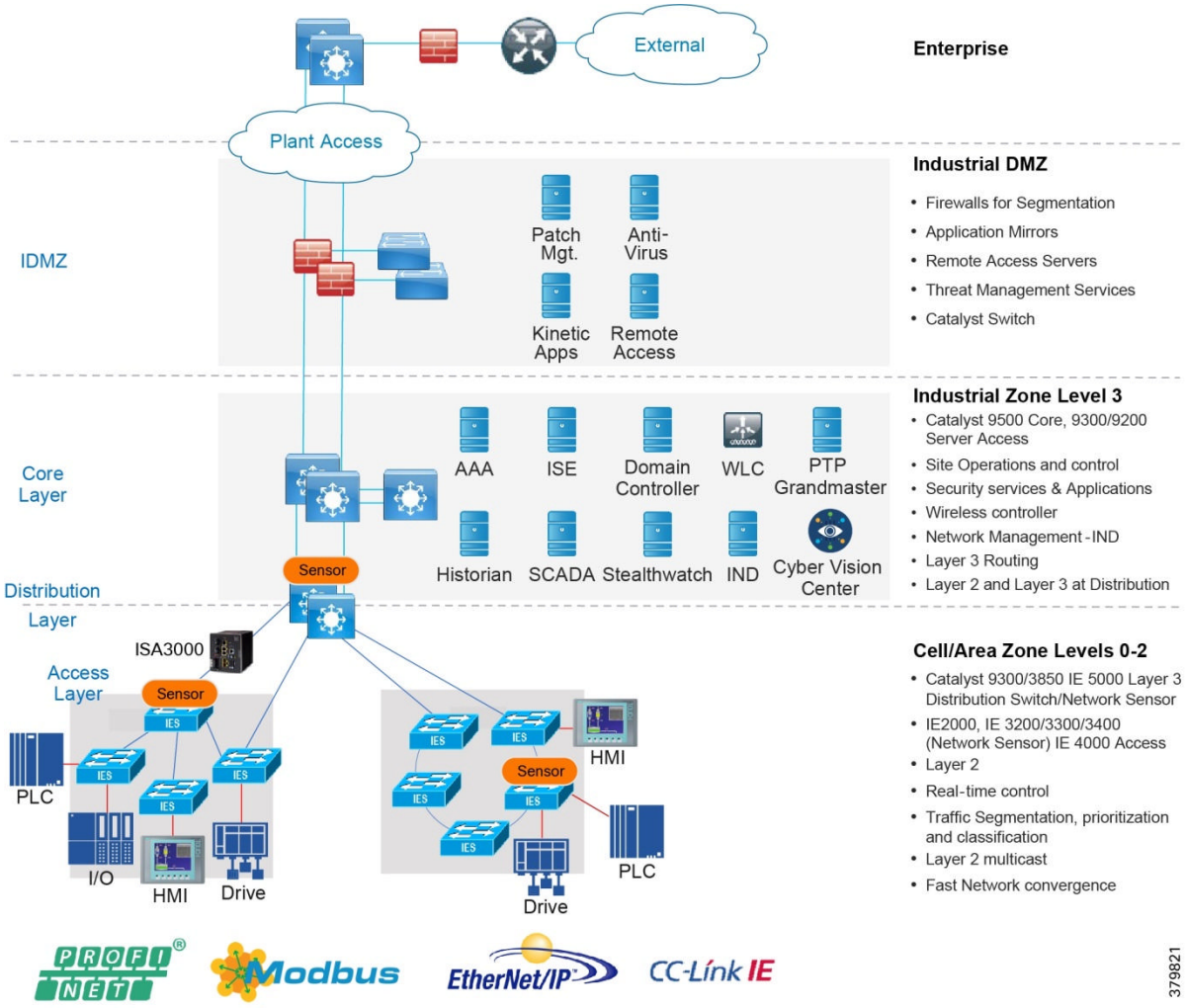


Рисунок 3.10 – Модель мережі промислової автоматизації та еталонна архітектура IACS.

4 СПЕЦІАЛЬНА ЧАСТИНА

Усі проекти великих мереж зі складною топологічною будовою на теперішній час не обходиться без детального моделювання проектованої мережі. Програми, котрі призначені для виконання даної задачі, складні й вартісні. Мета створення моделі мережі є визначення оптимальних топологій, відповідний вибір мережевого обладнання, визначення робочих параметрів й можливих етапів розвитку та масштабування мережі.

Моделювання використовують для дослідження характеристик нових модифікацій протоколів, методи роботи із чергами, для оптимізації параметрів якості обслуговування.

На етапі моделювання випробовують вплив пікових навантажень, великих потоків запитів. Моделювання дозволяє імітувати режими колапсу мережі (для Ethernet), що навряд можна відтворити у працюючій мережі. Процес створення моделі мережі встановлює наступні параметри:

- граничні пропускні здатності;
- залежності втрат пакетів від завантаження;
- визначає прогнозований час відгуку у різних режимах;
- оптимізує конфігурацію;
- визначає вплив масштабування мережі та перерозподілення інформаційних потоків (встановлення додаткових Proxy, Firewall і т.д.);
- оптимізує топологію мережі (локацію зовнішніх шлюзів, серверів, DNS , організацію опорних каналів та ін.);
- вибір типів мережевого обладнання та режимів його роботи ;
- вибір протоколів внутрішньої маршрутизації їх параметрів;
- визначає гранично припустиме число абонентів того або іншого сервера;
- оцінює необхідні смуги перепускання зовнішніх каналів для забезпечення необхідних рівнів QOS.
- оптимізує параметри системи обслуговування черг;

- оцінює вплив пікового трафіку на роботу LAN;
- здійсює вибір схеми опорної мережі і протоколів сервіс–провайдеру й т.д.

Завдання моделювання обробки черг у віртуальному каналі з метою оцінки параметрів якості обслуговування вимагають не настільки значних ресурсів. Але з урахуванням перебору можливих значень параметрів конфігурації це також може зайняти багато годин.

У випадку моделювання реальної мережі можна зробити відповідні виміри, що іноді теж не занадто просто. З огляду на складність моделювання, варто обмежуватися моделюванням не більш ніж один хвилини для кожного з наборів параметрів (цього часу досить для копіювання практично будь–якого файлу через локальну мережу). Виключення може становити моделювання зовнішнього трафіку, але в цьому випадку весь локальний трафік повинен розглядатися як фоновий. Сучасні розподілені технології дають нові можливості для рішення завдань моделювання.

4.1 Аналітичне моделювання

Визначення характеристик мережі до того, як вона буде уведена в експлуатацію, має першорядне значення. Це дозволяє відрегулювати характеристики локальної мережі на стадії проектування. Рішення цієї проблеми можливо шляхом аналітичного або статистичного моделювання. По суті, у даному розділі мова йде про опис мережі в рамках теорії масового обслуговування.

Аналітична модель мережі являє собою сукупність математичних співвідношень, що зв'язують між собою вхідні й вихідні характеристики мережі. При виводі таких співвідношень доводиться зневажати якимись малоістотними деталями або обставинами.

Телекомунікаційна мережа при деякому спрощенні може бути представлена у вигляді сукупності процесорів (вузлів), з'єднаних каналами зв'язку. Повідомлення, що прийшло у вузол, якийсь час перебуває в черзі до

того, як воно буде оброблено. Час передачі або повний час затримки повідомлення D дорівнює:

$$D = T_p + S + W,$$

де T_p, S і W відповідно — час поширення, час обслуговування й час очікування. Однієї із завдань аналітичного моделювання є визначення середнього значення D. При більших завантаженнях основний внесок дає очікування обслуговування W. Для опису черг надалі буде використана анотація Д. Дж. Кенделла:

$$A/B/C/K/m/z,$$

де A — процес прибуття: B — процес обслуговування; C — число серверів (вузлів); K — максимальний розмір черги (за замовчуванням — ∞); m — число клієнтів (за замовчуванням — ∞); z — схема роботи буфера (за замовчуванням FIFO). Букви A и B представляють процеси приходу й обслуговування й звичайно заміняються наступними буквами, які характеризують закон, що відповідає розподілу подій:

- D — постійна ймовірність;
- M — марковський експонентний розподіл;
- G — узагальнений закон розподілу;
- E_k — розподіл Ерланга порядку k;
- H_k — гіперекспонентний розподіл порядку k.

Найпоширенішими схемами роботи буферів є FIFO (First–In–First–Out), LIFO (Last–In–First–Out) і FIRO (First–In–Random–Out). Наприклад, запис M/M/2 означає черга, для якої часи приходу й обслуговування відповідає експонентному розподілу, є два сервери, довжина черги й число клієнтів можуть бути як завгодно більшими, а буфер працює за схемою FIFO. Середнє значення довжини черги Q при заданій середній вхідній частоті повідомлень λ і середньому часі очікування W визначається на основі *теореми Літла* (1961):

$$Q = \lambda \times W$$

Для варіанта черги M/G/1 вхідний процес характеризується розподілом Пуассона зі швидкістю надходження повідомлень λ. Імовірність надходження k повідомлень на вхід за час t дорівнює:

$$p(k) = \frac{(\lambda t)^k}{k!} e^{-\lambda t},$$

k=0,1,2,...

Нехай N — число клієнтів у системі, Q — число клієнтів у черзі, і нехай імовірність того, що вхідний клієнт виявить j інших клієнтів, дорівнює:

$$\Pi_j = P[n = j], j = 0, 1, 2, \ldots \sum_{j=0}^{\infty} \Pi_j = 1; \Pi_0 = 1 - \rho; \rho = \lambda\tau$$

Тоді середній час очікування w:

$$\overline{W} = \frac{\overline{Q}}{\lambda} = \frac{\rho\tau}{2(1-\rho)}\left(1 + \frac{\sigma^2}{\tau^2}\right)$$

(Формула Поллажека–Хінчіна).

σ – середньоквадратичне відхилення для розподілу часу обслуговування.

Для варіанта черги M/G/1 $H(t) = P[X \leq t] = 1 - e^{-\mu t}$ (H — функція розподілу часу обслуговування). Звідки треба $\sigma^2 = \tau^2$.

$$\overline{W} = \frac{\rho\tau}{(1-\rho)}$$

Для варіанта черги m/d/1 час обслуговування постійно, а середній час очікування становить:

$$\overline{W} = \frac{\rho\tau}{2(1-\rho)}$$

Аналітична модель для мереж Ethernet (CSMA–CD) розроблена Лемом («S.S.Lam: A Carrier Sense Multiple Access Protocol for Local Networks, Computer Networks, vol. 4, n. 1, pp. 21–32, January 1980»). Тут передбачається, що мережа складається з нескінченного числа станцій, з'єднаних каналами з доменним доступом. Тобто станція може почати передачу тільки на початку якогось часового домену. Розподіл повідомлень підкоряється закону Пуассона з

постійною швидкістю проходження λ. Середнє значення часу очікування для таких мереж становить:

$$\overline{D} = \frac{\lambda[S^2 + (+e+2)\tau S + 5\tau^2 + +e(2e-1)\tau^2]}{2(1-\lambda[\overline{S} + \tau + 2e\tau])} - \frac{(1-e^{-2\lambda\tau})(e+\lambda\tau-2\lambda\tau e)}{\lambda e[F(\lambda)e^{-(1+\lambda\tau)} + e^{-2\lambda\tau} - 1]} + 2\tau e + \overline{S} + \tau/3$$

де e — підстава натурального логарифма, τ — затримка поширення сигналу в мережі. S і S^2 — відповідно перший і другий моменти розподіли передачі або обслуговування повідомлення. f(λ) перетворення Лапласа для розподілу часу передачі повідомлення. Отже,

$$F(\lambda) = \int_0^{\infty} f(t)e^{-\lambda t}, dt$$

а для повідомлень постійної довжини $f(\lambda)=e^{-\circ}$, $S^2=S^2$, де $\pi=\lambda S$. Для експонентного розподілу довжин повідомлень:

$$F(\lambda) = \frac{1}{1+\rho}, \overline{S^2} = 2\overline{S}^2$$

Розглянемо варіант мережі Ethernet на основі концентратора–перемикача із числом каналів N. При цьому буде передбачатися, що повідомлення на вході всіх вузлів мають пуассонівський розподіл із середньою інтенсивністю λ_i, а розподіл повідомлень по довжині довільно. Повідомлення відправляються в тім же порядку, у якому вони прибули. Трафік у мережі передбачається симетричним. Черга має модель M/G/1. Середній час очікування в цьому випадку дорівнює:

$$\overline{W} = \hat{y} + \frac{\lambda\hat{y}^2}{2(1-\rho)},$$

де $\hat{y} = [1 + (N-2)\rho G]\overline{S}$,

$$\hat{y}^2 = 2[1 + (N-2)\rho G + (N-2)(N-3)\rho^2 G^2]\overline{S^2}$$

$$\rho = \frac{\lambda S}{1-(N-2)G\lambda\overline{S}},$$

$\lambda=\lambda_i$, а G=1/(N–1) дорівнює ймовірності того, що повідомлення відправника i спрямовано одержувачеві j. Вимога стабільності $\rho \leq 1$ зобов'язує, щоб $\lambda S \leq$ (N–1)(2N–3)

Для більших n це приводить до $\lambda S \leq 1/2$.

Середній час поширення повідомлення в мережі дорівнює $T_p = \tau$, де τ дорівнює RTT.

$$\overline{D} = \hat{y} + \frac{\lambda \hat{y}^2}{2(1-\rho)} + \overline{S} + \tau$$

Особливе місце займає моделювання систем роботи із чергами. Ці завдання стали особливо актуальними у зв'язку необхідністю одержання гарантованих параметрів якості обслуговування. Цей тип моделювання можна реалізувати за допомогою загальнодоступної програми NS–2.

4.2 Симуляційне моделювання

Симуляційне або статистичне моделювання використовують для аналізу систем для виявлення критичних точок у мережі. Це моделювання використовують для прогнозування характеристик систем.

Симуляційне моделювання може здійснюватися з використанням спеціалізованих мов симулювання й вимагає апріорного знання щодо статистичних властивостей системи в цілому й окремих її елементах. Процес створення моделі містить – саме формування моделі, налагодження програми й перевірку адекватності отриманої моделі. Останній етап звичайно складається з порівняння розрахункових результатів з експериментальними даними, отриманими для реальної мережі.

При статистичному моделюванні необхідно задати ряд часових характеристик, наприклад: таблиця 2.1.

Таблиця 4.1 – Часові характеристики

Системний час	Інтервал від моменту генерації повідомлення до одержання його адресатом, включаючи очікування в черзі
Час очікування	Проміжок часу від прийому повідомлення мережним інтерфейсом до обробки його процесором
Час поширення	Затримка передачі повідомлення від одного мережевого інтерфейсу до іншого

Повний список таких часових характеристик містить у собі значно більше величин.

У процесі моделювання розраховуються наступні параметри:

Таблиця 4.2 – Параметри черг

Статистика черг
Середня довжина черги
Пікова довжина черги
Середньоквадратичне відхилення довжини черги від середнього значення
Статистика часу очікування
Середній час очікування
Максимальний час очікування
Середньоквадратичне відхилення часу очікування
Статистика системного часу
Середній системний час
Максимальний системний час
Середньоквадратичне відхилення системного часу

Продовження таблиці 2.2 .
Повне число повідомлень у статистику системного часу
Пікове значення числа системних повідомлень
Середньоквадратичне відхилення числа системних повідомлень
Статистика втрат повідомлень
Повне число загублених повідомлень
Частота втрати повідомлень
Частка втрат через переповнення черги
Частка втрат через таймаутів

Зрозуміло, реальний перелік параметрів, що обчислюються, може бути істотно ширше й визначається конкретними цілями розрахунків. Розглянемо приватне завдання визначення середнього числа зв'язків між процесорами (вузлами). Передбачається, що повне число вузлів дорівнює `N`, а схема з'єднання вузлів відповідає зображеної на рисунку 4.1.

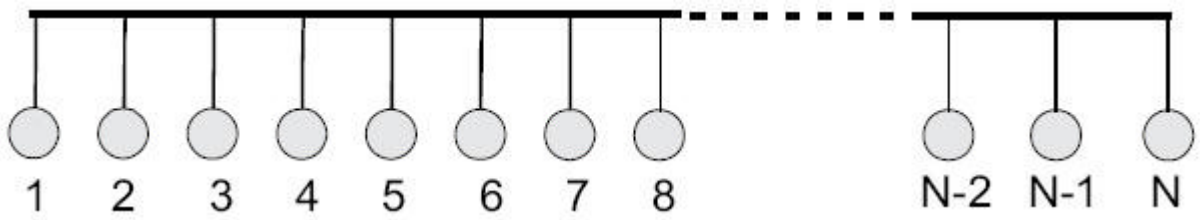


Рисунок 4.1 – Схема з’єднання вузлів

Середня відстань від довільного вузла до всіх інших вузлів дорівнює `D(N+1)/3`, де `D` — відстань між сусідніми вузлами (передбачається константою).

Можливі різні підходи до моделювання. Класичний підхід полягає у відтворенні подій у мережі як можна точніше й поетапному моделюванні наслідків цих подій.

У реальному житті події можуть відбуватися одночасно в різних точках мережі. Із цієї причини для моделювання ідеально підійшов би багатопроцесорний комп'ютер, де можна відтворювати будь–яке число процесів одночасно (сучасні розподілені обчислювальні системи для рішення таких завдань підходять ідеально). У кожному разі необхідно вибрати деякий постійний часовий інтервал і вважати, що події відбулися одночасно, якщо відстань між ними менше цього інтервалу.

Для мереж типу Ethernet таким часовим інтервалом може бути біт–такт (для 10–мегабітного Ethernet це 100нс). Зрозуміло, що це вже відступ від реальності (адже затримки в мережевому кабелі не кратні цьому часу), але не занадто значуще. Треба сказати, що такого роду припущень при моделюванні доводиться робити багато. Із цієї причини надто важливо порівнювати результати моделювання з даними, отриманими для реальної мережі. Якщо відмінності лежать у межах 10–20%, можна вважати, що зроблені припущення не повели програму занадто далеко від життя й нею можна користуватися для розрахунків. Розглянутий вище підхід придатний для моделювання мережевого колапсу, тому що швидкість розрахунків тут залежить від числа вузлів і майже не залежить від мережевого завантаження.

Іншим підходом може стати метод, де для кожного логічного сегмента (зони зіткнень) спочатку моделюється черга подій. При цьому в кожній робочій станції моделюється послідовність пакетів, що очікують відправлення. Ця черга може час від часу модифікуватися, наприклад, при одержанні ЕОМ пакета ззовні й необхідності послати на нього відгук. Після того як така черга для кожного мережевого об'єкта (сюди, крім ЕОМ, входять мости, перемикачі й маршрутизатори) побудована, запускається програма відправлення пакетів: вибирається найперший за часом пакет (що очікує довше інших) і перевіряються для нього умови початку передачі (відсутність несучої на вході мережевого інтерфейсу в цей момент і протягом попередній 96 біт–тактів). Якщо умови відправлення виконані, пакет посилає в мережу. Обчислюються

моменти досягнення їм всіх вузлів даного логічного сегмента, перевіряються умови його зіткнення з іншими пакетами. Варто помітити, що в цьому підході знімаються обмеження дискретності часової шкали, використаної в попередньому "класичному" підході. Цей підхід дозволяє помітно прискорити розрахунки при великій кількості вузлів, але малому завантаженню мережі. Проблеми реалізації даної концепції моделювання пов'язані з обслуговуванням досить складного списку, що описує черга пакетів, що очікують відправлення. У структуру цього списку включається й опис ситуації в мережі на даний часовий період. Додаткові труднощі сполучені з поведінкою мостів, перемикачів і маршрутизаторів, тому що вони можуть вставляти в чергу додаткові елементи, що вимагають негайного обслуговування. Аналогічні вставки в чергу будуть викликати отримані станцією пакети ICMP або TCP, що вимагають відгуків. Причому таке вставляння в чергу асинхронно стосовно процедури "відправлення" пакетів. Черга для всієї локальної мережі може бути єдиною, тоді пакети різних логічних сегментів повинні бути позначені певними прапорами. При переході із сегмента в сегмент прапор буде мінятися. Можливо й побудова незалежних черг для кожного з логічних мережевих сегментів.

Такі режими важко реалізувати на практиці без завдання серйозних збитків клієнтам мережі. Результати розрахунку представлені на рисунку 2.2. Метою моделювання є визначення залежності пропускної здатності мережі й імовірності втрати пакета від завантаження, числа вузлів у мережі, довжини пакета й розміру області зіткнень.

Вихідні дані про структуру й параметри мережі беруться з бази даних. Ряд параметрів мережі задаються конфігураційним файлом (профайлом). Сюди можуть записуватися ємність буфера інтерфейсу й драйвера, час затримки обробки запиту (хоча в загальному випадку ця величина може також мати розподіл) і т.д.. До таких параметрів ставляться також: MTU, MSS, TTL, window, деякі значення таймаутів і т.д.

Мережа розбивається на логічні сегменти, у кожному з яких працює незалежна синхронізація процесів (хоча ці процеси й впливають один на одного через мости, перемикачі й маршрутизатори).

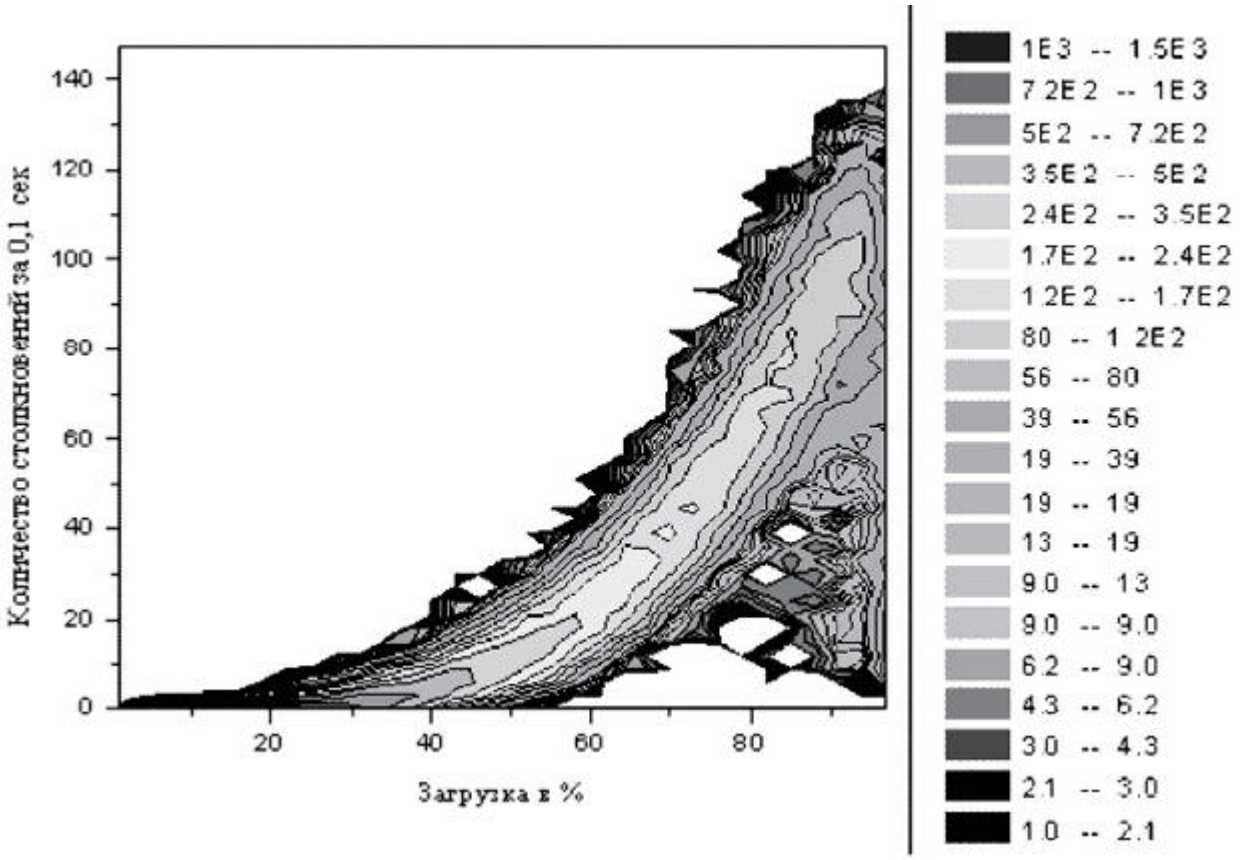


Рисунок 4.2 – Залежність імовірності втрати пакета у відсотках від завантаження фрагмента мережі

Повне моделювання мережі з урахуванням робочих додатків припускає використання наступних розподілів:

- розподіл по відсотку часу використання кожного з вузлів для того або іншого виду додатків;
- розподіл вузлів мережі по їхній активності;
- розподіл по використовуваних протоколах;
- розподіл по довжинах пакетів.

Останні два пункти істотно корельовані з першим, тому що використовувані протоколи залежать від додатка, а активність вузла може визначатися, наприклад, довжиною файлу, що пересилається. Із цієї причини

при повномасштабному моделюванні спочатку визначається, що збирається робити робоча станція або сервер (з урахуванням розподілу по додатках визначається характер завдання: FTP, MS explorer і т.д.). Потім розігруються параметри завдання (довжина файлу, далекість об'єкта та ін.), а вже на основі цього формується фрагмент черги пакетів.

Завдання першого етапу: перевірка пропускної здатності при варіації завантаження й довжин пакетів, підрахунок числа зіткнень (якщо вони можливі), перевірка впливу розміру буфера мережевого інтерфейсу на пропускну здатність (вплив розміру буфера перемикачів по шляху до адресата).

Вихідні дані для першого етапу:

- частота посилки пакетів для кожного з вузлів (на початку рівна для всіх) [δ — інтервал між пакетами];
- довжина пакета, що посилається кожним вузлом, (на початку дорівнює для всіх: мінімальна [512 біт] і максимальна [12000 біт];
- часовий розподіл моментів посилки пакетів (на початку рівномірний).

Структура опису кожного з вузлів містить у собі (формується з урахуванням майбутнього розширення):

- номер вузла (ідентифікатор);
- код типу вузла (байт: робоча станція, міст, перемикач, маршрутизатор, повторювач);
- MAC–Адреса (для повторювача =0);
- IP–Адреса (для повторювача, звичайного MAC–Моста й перемикача =0);
- байт статусу (вузол веде передачу; до вузла дійшов чужий пакет;....);
- δ— середня відстань між кінцем попередні й початком чергового пакета в біт–тактах;
- дисперсія ширини пакетів;
- дисперсія значення δ(зазор між послідовними пакетами);
- код використовуваного протоколу (IPv4 або IPv6; TCP, UDP, ICMP і т.д.);
- повна довжина повідомлення в байтах;

- час обробки пакета (затримка посилки відгуку в біт–тактах);
- довжина чергового пакета;
- байт типу адресації (unicast, broadcast, multicast);
- ширина вікна (число пакетів, що відправляються, без підтвердження, для TCP);
- обсяг вхідного буфера (число пакетів; може вимірятися й у байтах, але тоді потрібні спеціальні покажчики). Тип буфера (FIFO, LIFO і т.д.);
- обсяг вихідного буфера (число пакетів);
- байт режиму роботи (для мостів і перемикачів: cut–through; store–and–forward і т.д.; для робочої станції визначається типом використовуваного протоколу й фазою його реалізації).

Формат опису топології мережі (список) Елемент списку:

- ідентифікатор вузла (номер);
- код типу вузла;
- список вузлів сусідів (номер_сусіда (ідентифікатор): затримка_до_його).

Процес посилки пакета містить у собі (відповідно до вимог документа IEEE 802.3):

1. перевірку можливості початку (відсутня чужа активність, ipg=96 біт–тактів);
2. послідовну передачу бітів (кожний біт–такт);
3. контроль стану зіткнень (якщо зіткнення можливо);
4. обробка випадків зіткнення (посилка jam);
5. при зіткненні обчислення номера біт–такту спроби поновлення передачі.

Спроба початку передачі припускає перевірку:

1. чи здійснювалася передача на попередній біт–такті;
2. контролю числа вільних від передачі біт–тактів (<96 ?).

Процес прийому припускає:

1. контроль закінчення прийому (біт–такт без даних у каналі). Закінчення прийому може означати перехід у режим аналізу отриманих даних;

2. контроль наявності зіткнення;
3. необхідність передбачити можливість (у деяких режимах) контролю адрес (MAC і IP) і вмісту пакета й т.д. (включаючи зміну режиму роботи вузла, наприклад, перехід від читання до передачі). Даний пункт абсолютно необхідний для мостів і перемикачів.

Центральний менеджер здійснює:

1. реєстрацію початку передачі кожним з вузлів (номер вузла й номер біт–такту);
2. розрахунок положення початку пакета до початку черговий біт–такту для всіх можливих шляхів поширення;
3. запис статусу вузлів

Рівномірний розподіл за часом

Для кожного вузла встановлюється певна середня частота посилки пакетів. Час початку сесії передбачається випадковим. Середня частота може бути задана рівної для всіх вузлів.

Мінімальний середній період посилки пакетів визначається в біт–тактах і повинен бути більше 512 біт–тактів. Зрозуміло, що поки вузол здійснює передачу, він не може намагатися передати новий пакет. Із цієї причини частота посилки пакетів однозначно визначається паузою між кінцем попереднього пакета й початком нового (δ). Середнє значення періоду посилки пакетів дорівнює $T_{пакета}$+96(біт-тактів)+δ (значення δвеличина в загальному випадку статистична). Для кожного вузла задається значення δ(спочатку рівне для всіх вузлів). Якщо припустити рівномірний розподіл імовірності, передача пакета може початися в будь–який біт–такт із рівною ймовірністю.

При визначенні того, чи намагатися починати передачу в даний біт–такт, буде зроблена перевірка умови:

rndm<1/δ (виконання умови припускає спробу початку передачі).

Якщо ймовірність приходу n пакетів на час t розподілена за законом Пуассона:

$$P = \frac{(Lt)^n e^{Lt}}{n!},$$

де L — середня частота проходження подій, то реальний час між подіями може бути визначене як τ = −T ln(R). R — випадкове число 0 ≤R ≤1, а T = 1/L.

Результатами моделювання можуть бути (фіксуються окремо для кожного набору вхідних параметрів): таблиця 2.3.

Таблиця 2.3

Результати моделювання

1.	Імовірність втрати пакета для логічного сегмента й кожної з робочих станцій
2.	Пропускна здатність серверів для кожного з логічних сегментів (шлях сервер –> логічний сегмент)
3.	Імовірність зіткнення для кожного логічного сегмента й кожної робочої станції
4.	Розподіл потоків по логічних сегментах (і робочим станціям) незалежно для кожного напрямку (вхід і вихід)
5.	Розподіл потоків для всіх входів/виходів перемикачів мостів і маршрутизаторів
6.	Частка допоміжного трафіка (ICMP, SNMP, відгуки TCP, широкомовні запити й т.д.) стосовно інформаційного потоку для різних вузлів мережі (серверів, маршрутизаторів)
7.	Рівень широкомовного трафіка для кожного з логічних сегментів

Набір параметрів, розподілів і алгоритм моделювання сильно залежить від вартого завдання.

4.3 Мережеві драйвери

При знайомстві з телекомунікаційними протоколами, виникає питання, як писати прикладні програми для роботи з пакетами. У більшості випадків цілком достатньо скористатися стандартною бібліотекою для роботи із сокетами. В особливих випадках може виникнути необхідність одержання даних безпосередньо від мережевого інтерфейсу.

Прикладна програма взаємодіє із драйвером мережевого інтерфейсу. Ethernet–Інтерфейс, як і всі інші, містить кілька статусних керуючих регістрів: (CSR – ControlStatusRegister) і один або кілька регістрів даних. Запис (читання) у ці регістри виконується в IBM/PC за допомогою команд IN (OUT). Кожному регістру ставиться у відповідність певний номер порту. Блок номерів портів задається в процесі постановки пакетного драйвера.

Варто мати на увазі, що різні інтерфейси можуть мати різне число CSRм–регістрів і відмінні від наведених нижче функції (NE2100). Інтерфейс характеризується трьома цілими числами: клас (8 біт), тип (16 біт) і номер. Клас говорить про те, для якої з мережевих середовищ призначений даний прилад (PPP, DIX Ethernet, IEEE 802.3, IEEE 802.5, Pronet–10, Appletalk і т.д.). Тип описує конкретну реалізацію інтерфейсу (NE2100, NI5210, 3C501 і т.д.). Тип 0xffff відповідає всім інтерфейсам даного класу. У випадку, коли ЕОМ оснащена більш ніж одним інтерфейсом ідентичного типу, для їхньої ідентифікації використовується номер. На рисунку 4.3 показано структуру керуючого (*CSR*) регістра мережевого інтерфейсу.

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Init	Strt	Stop	Tdnd	Txon	Rxon	Inea	Intr	Idon	Tint	Rint	Merr	Miss	Cerr	Babl	Err

Рисунок 4.3 – Структура CSR–Регістра інтерфейсу (CSR0).

Таблиця 2.4 – Структура CSR–Регістра інтерфейсу

Init	ініціалізація (initialize)
Strt	старт
Stop	стоп
Tdnd	запит передачі (transmit demand)
Txon	включення передачі
Rxon	включення прийому
Inea	дозвіл переривань (interrupt enable)
Intr	переривання
Idon	ініціалізація виконана (стирання записом 1)
Tint	переривання при передачі (стирання записом 1)
Rint	переривання при читанні (стирання записом 1)
Merr	помилка при тайм–ауті на шині (стирання записом 1)
Miss	ні буфера для прийому (стирання записом 1)
Cerr	помилка через зіткнення (стирання записом 1)
Babl	тайм–аут при передачі (стирання записом 1)
Err	помилка типу Babl, Cerr, Miss, Merr (тільки для читання)

*CSR*1 (доступ дозволений при *CSR*0[stop] = 1)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Старшие 8 бит адреса блока IADDR								0	0	0	0	0	0	0	0

Рисунок 4.4 – CSR1

CSR2 (доступ дозволений при CSR0[stop] = 1)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	Младшие 15 бит адреса блока инициализации (IADDR)														

Рисунок 2.5 – CSR2

Bcon 0 = <0:7> перестановка байтів адрес

Acon 0 = ale, 1 = /as

Bswp 0 = /bm1, bm0, /hold;

*CSR*3 (доступ дозволений при *CSR*0[stop] = 1)

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Bcon	Acon	Bswp	0	0	0	0	0	0	0	0	0	0	0	0	0

Рисунок 2.6 – CSR*3*

Структура змінних init_mode (зсув = 0) має вигляд

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Drx	Dtx	Loop	Dtcr	Coll	Dtry	Intl	0	0	0	0	0	0	0	0	Prom

Drx заборона прийому

Dtx заборона передачі

Loop цикл

Dtcr заборона передачі CRC

Coll зіткнення

Drty заборона повторів

Intl внутрішній цикл

Prom режим прийому всіх пакетів (promiscuous mode)

Рисунок 2.7 – Структура змінних init_mode

Наведений вище опис регістрів інтерфейсу не є єдино можливим. Структура драйверів варіюється для різних операційних систем. Для системних програмістів корисно мати можливість набудовувати драйвер або безпосередньо інтерфейс на певний режим, наприклад, на прийом всіх пакетів, що проходять по кабельному сегменті. Останнє може становити інтерес у діагностичних цілях, тому що слідом за пакетним драйвером завантажується Etherdrv, Winsock або winpkt і т.д., що блокують режим прийому всіх пакетів (mode=6).

Існує безліч пакетних драйверів. Можна виявити кілька модифікацій для того самого типу інтерфейсу. Ці драйвери можуть бути орієнтовані на роботу в різних програмних середовищах і мати різні можливості. Драйвер може використовувати мінімум можливостей інтерфейсу (базовий рівень), реалізувати більше широкий набір функцій (мультикастинг, збір статистики й т.д.) або підтримувати практично всі, на що здатен даний інтерфейс. В останньому випадку він займає більше місця в пам'яті. При написанні програми варто пам'ятати, що порядок байтів в Ethernet протилежний тому, що використовується у вашій машині.

Пакетні драйвери використовують програмні переривання в інтервалі `0x60 – 0x80`. Варто відразу помітити, що не всі переривання із цього списку вільні, і при лихословити системи варто проявляти обачність. Для того, щоб уникнути конфліктів з іншими зовнішніми пристроями, передбачається можливість реконфігурації переривань. Практично всі драйвери можуть працювати з різними протоколами (TCP/IP, OSI і ін.). Вирішити завдання націлити на зв'язному рівні допомагає процедура access_type, що забезпечує доступ для пакетів певного типу.

Всі функції реалізуються за допомогою звертання до драйвера з набором певних параметрів. Кожному типу використовуваного мережевого протоколу, з яким працює інтерфейс, ставиться у відповідність цілочислового покажчика (handle), одержуваного за допомогою процедури access_type. Виконуваність

драйвером тих або інших операцій може бути з'ясована за допомогою запиту driver_info.

Варто пам'ятати, що порядок байтів в PC і в деяких мережах, включаючи Ethernet, не збігається. Мультикастинг адресація реалізується на рівні L2, при цьому список мультикаст–адрес підписки користувачів зберігається в мережевому інтерфейсі й може бути прочитаний по запиті.

Сучасні мережеві інтерфейси роблять підрахунок прийнятих і переданих октетів, кількість різного типу помилок та ін. Одержання статистичних даних про помилки й трафік через даний інтерфейс здійснюється за допомогою запиту get_statistics(handle). Статистичні дані мають вигляд цілих 32–розрядних чисел. Практично всі інтерфейси допускають зміну MAC–Адреси, що прошили виготовлювачі інтерфейсу.

5 НАУКОВО–ДОСЛІДНИЦЬКА ЧАСТИНА

5.1 Керування множинним доступом у централізованих мережах передачі даних

Активний розвиток мереж передачі даних спричиняється необхідність дослідження розповсюдженого методу, використовуваного при передачі в цих мережах – множинного доступу абонентів до загального каналу зв'язку. Множинний доступ припускає поділ ресурсів каналу між абонентами. Такий поділ каналів може бути частотним, часовим або кодовим. Множинний доступ застосовується й у провідні й у бездротових мережах. Розрізняють безконфліктні й конфліктні методи доступу. Безконфліктні методи множинного доступу використовують у стільникових мережах стандартів AMPS, NAMPS, GSM (у режимі передачі мови) і інших. Серед конфліктних методів доступу широке поширення отримав стандарт для локальних провідних мереж IEEE 802.3 (Ethernet) і стандарт для локальних бездротових мереж – IEEE 802.11. У цей час іде активне впровадження стандарту для бездротових MAN–Мереж – IEEE 802.16. Даний стандарт, як і стандарт для провідних мереж IEEE 802.14, характеризується наявністю центральної станції. Особливістю стандартів IEEE 802.16 і IEEE 802.14 для мереж із центральною станцією (централізовані мережі) є використання конкурентного інтервалу в процесі передачі. У конкурентному інтервалі абоненти передають запити до центральної станції на надання канальних ресурсів. Абонент передає запит випадковим образом. Якщо передачі запитів від різних абонентів накладаються один на одного, то виникає конфлікт. У цьому випадку абоненти роблять повторну передачу відповідно до певних правил. І так далі. Ясно, що правила керування передачею в конкурентному інтервалі можуть дуже впливати на затримку передачі запиту. А це, в остаточному підсумку, вплине на час, що затратить абонент на передачу даних. Магістерська робота присвячена дослідженню алгоритмів керування

передачею в конкурентному інтервалі, які прийнято називати алгоритмами випадкового множинного доступу. Основна ідея методу випадкового множинного доступу (ВМД) запропонована на початку 70–х років минулого століття й розвинена в роботах Капетанакіса, Цибакова, Михайлова, Мессі й ін. Спеціально для централізованих мереж в 1999 році Блонді й іншими розроблений алгоритм ВМД, що отримав назву «FS–ALOHA».

Метою роботи є розробка й аналіз алгоритмів керування передачею запитів у конкурентному інтервалі, що використовують випадковий множинний доступ і забезпечують оперативну доставку запитів на центральну станцію.

Завданнями дослідження є:

1). Аналіз функціонування відомого алгоритму ВМД із чергою для централізованих мереж.

2). Розробка алгоритмів ВМД, що забезпечують меншу затримку при доставці запиту, чим раніше відомі алгоритми.

3). Аналіз запропонованих алгоритмів для різних видів вхідного потоку.

Методи дослідження. Для рішення поставлених завдань використані методи теорії ймовірностей, теорії випадкових процесів, теорії ланцюгів Маркова, методи теорії масового обслуговування й імітаційне моделювання.

Основні положення, що досліджуються у розділі.

– метод розрахунку швидкості й метод розрахунку розподілу ймовірностей для затримки запиту в алгоритмі FS–ALOHA у каналі із шумом;

– алгоритм керування передачею запиту в конкурентному інтервалі централізованих мереж – Multi FS–ALOHA;

– клас алгоритмів ВМД для централізованих мереж. Метод розрахунку швидкості й метод вибору оптимальних параметрів для підкласу алгоритмів ВМД.

Наукова новизна проведених досліджень.

1). Розроблено метод розрахунку швидкості алгоритму FS–ALOHA для каналу із шумом, що приводить до появи помилкових конфліктів.

2). Обчислено критичне значення ймовірності помилкового конфлікту, при якому швидкість для оптимальних щодо швидкості параметрів алгоритму FS–ALOHA дорівнює нулю.

3). Розроблено метод розрахунку розподілу ймовірностей для затримки передачі запиту в алгоритмі FS–ALOHA у каналі із шумом.

4). Запропоновано клас алгоритмів ВМД із чергою для централізованих мереж.

5). Розроблено метод обчислення швидкості алгоритму для підкласу алгоритмів ВМД із запропонованого класу. Розроблено метод визначення параметрів алгоритму з даного підкласу, при яких його швидкість максимальна. Розроблено метод обчислення швидкості при вхідному потоці зі сплесками інтенсивності для алгоритмів з підкласу.

Практична цінність.

1). Запропоновано модифікацію алгоритму FS–ALOHA – алгоритм Multi FS–ALOHA. Модифікація вирішила проблему зменшення швидкості в алгоритмі FS–ALOHA при збільшенні розміру конкурентного інтервалу.

2). Запропоновано деревоподібні алгоритми ВМД для централізованих мереж. Дані алгоритми мають більшу швидкість у порівнянні з Multi FS–ALOHA, але при цьому мають і більшу обчислювальну складність.

3). Отримано чисельні значення характеристик алгоритму FS–ALOHA у каналі із шумом. Чисельні характеристики розраховані для запропонованих алгоритмів ВМД при різних значеннях їхніх параметрів.

4). Зроблено порівняння алгоритму BEB, використовуваного в стандарті IEEE 802.16, з одним з деревоподібних алгоритмів ВМД для централізованих мереж.

5.2 Особливості підрівня керування доступом до середовища в централізованих мережах передачі даних

У даному розділі опишемо особливості підрівня керування доступом до середовища в централізованих мережах передачі даних на прикладі стандарту IEEE 802.16. Наведено модель системи, використовувана для аналізу функціонування алгоритмів ВМД. Визначено основні характеристики алгоритмів. Зроблено огляд використовуваних для централізованих мереж алгоритмів ВМД, а також деревоподібних алгоритмів дозволу конфліктів. Отримано оцінки характеристик алгоритму BEB у каналі із шумом і в каналі зі сплесками інтенсивності вхідного потоку.

Структура централізованої системи припускає поділ загального каналу зв'язку між абонентськими станціями (АС) і центральною станцією (ЦС) на два підканала: висхідні канали й спадний канал. Висхідний канал множинного доступу служить для передачі даних від абонентських станцій до центральної станції. АС «не чують» один одного. Комунікація між ними здійснюється за допомогою ЦС. Спадний канал призначений для передачі даних від ЦС до АС. Передача відбувається в широкомовному режимі. Тому її «чують» всі АС.

Організація передачі в централізованій системі відбувається шляхом поділу часу передачі на кадри, що мають певну структуру (мал. 5.1). АС передають дані за допомогою пакетів, які крім самих даних містять також поле з адресою одержувача, контрольну суму й іншу інформацію. Їхнє відправлення відбувається в інтервалі передачі пакетів висхідного каналу. Цей інтервал розбитий на відрізки часу, рівні тривалості передачі одного пакета. Конкурентний інтервал кадру необхідний АС для відправлення запитів про надання їм місця в інтервалі передачі пакетів. Конкурентний інтервал також розбитий на рівні відрізки часу (слоти), у кожний з яких може бути переданий один запит від АС. Отримавши запити, ЦС виносить рішення про те, які слоти

в інтервалі передачі пакетів будуть виділені для АС, і передає своє рішення в заголовку наступного кадру.

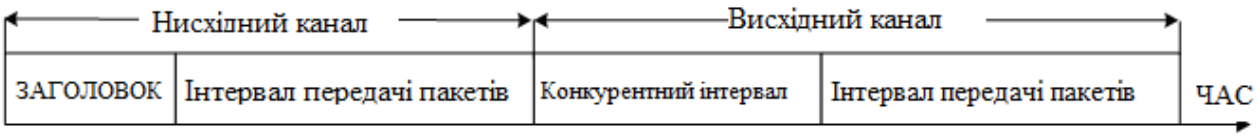


Рисунок 5.1 – Загальна структура кадру

Модель ВМД централізованої мережі полягає в наступному:

– розглядається тільки конкурентний інтервал;

– у слотах можлива або ситуація «порожньо» – передачі були відсутні, або ситуація «успіх» – відбулася успішна передача, або ситуація «конфлікт» – відбулася одночасна передача двох або більше запитів;

– АС одержують інформацію про ситуації в слотах на початку наступного кадру;

– кожна АС не може мати більше одного запиту в один момент часу.

Як модель шумів використовується модель помилкових конфліктів, повністю обумовлена двома ймовірностями: q_0 – імовірність, з якої ЦС через шум сприймає слот із ситуацією «порожньо» як слот із ситуацією «конфлікт» і q_1 – імовірність, з якої ЦС через шум сприймає слот із ситуацією «успіх» як слот із ситуацією «конфлікт». Шуми в спадному каналі відсутні (у припущенні великої потужності передавача ЦС).

Застосовуються дві моделі надходження запитів у систему. У першій моделі число вступників запитів розподілено за законом Пуассона з параметром λ, що визначає інтенсивність надходження запитів розраховуючи на кадр. Друга модель описується дискретним пачковим Марківським вхідним процесом (D–BMAP).

Алгоритм ВМД розглядається як алгоритм, що вирішує два завдання:

– завдання керування передачею нових запитів (за дане завдання відповідає алгоритм доступу до каналу);

– завдання керування повторною передачею запитів після виникнення конфліктів (це завдання вирішує *алгоритм дозволу конфліктів (АДК)).*

Використовуються наступні визначення основних характеристик алгоритмів ВМД, уведені Б.С. Цибаковим.

Затримкою запиту називається час від моменту виникнення запиту до моменту його успішної передачі (одиниця часу – один кадр).

Нехай у довільний момент часу t на яку–небудь ненавантажену абонентську станцію вводять запит, затримку якого позначимо через δ_t.

Середньою віртуальною затримкою запиту називається величина

$$D \triangleq \lim_{t\to\infty} \sup M[\delta_t]. \qquad 5.1$$

Швидкість *R* алгоритму ВМД – це верхня грань інтенсивності вхідного потоку, для якої середня затримка кінцева:

$$R \triangleq \sup_{\alpha}\{\alpha : D(\alpha) < \infty\}, \qquad 5.2$$

де $D(\alpha)$ – середня затримка при інтенсивності α запитів вхідного потоку розраховуючи на слот конкурентного інтервалу.

5.3 ВМД із чергою для централізованих мереж – FIFO by Sets ALOHA (FS–ALOHA).

Розглянемо відомий алгоритм ВМД із чергою для централізованих мереж – FIFO by Sets ALOHA (FS–ALOHA). Алгоритм є базовим стосовно інших алгоритмів ВМД із чергою, які досліджуються в магістерській роботі.

В FS–ALOHA всі L слотів конкурентного інтервалу розбиті на дві непересічні підмножини. Перша підмножина містить S *слотів доступу*, друга – $N = L - S$ *слотів дозволу конфліктів*. Першу спробу передачі запиту абоненти роблять випадковим образом за допомогою рівномірного вибору в одному зі S слотів доступу. Запити, які не були успішно передані в слотах доступу одного кадру, утворять конфліктну підмножину (КП). Дане КП стає в кінець черги з таких же КП, які очікують обслуговування. Передача запитів із КП відбувається випадковим образом за допомогою рівномірного вибору в

одному зі N слотів дозволу конфліктів. КП перебуває на початку черги доти, поки всі його запити не будуть успішно передані. Якщо черга порожня, то всі L слотів конкурентного інтервалу використовуються для передачі нових запитів. Приклад передачі запитів за допомогою алгоритму FS–ALOHA показаний на малюнку 5.2. На малюнку використані наступні позначення: в – успішна передача, до – конфліктна передача, A_i – абонент із номером i і овал із цифрами – КП із номерами абонентів.

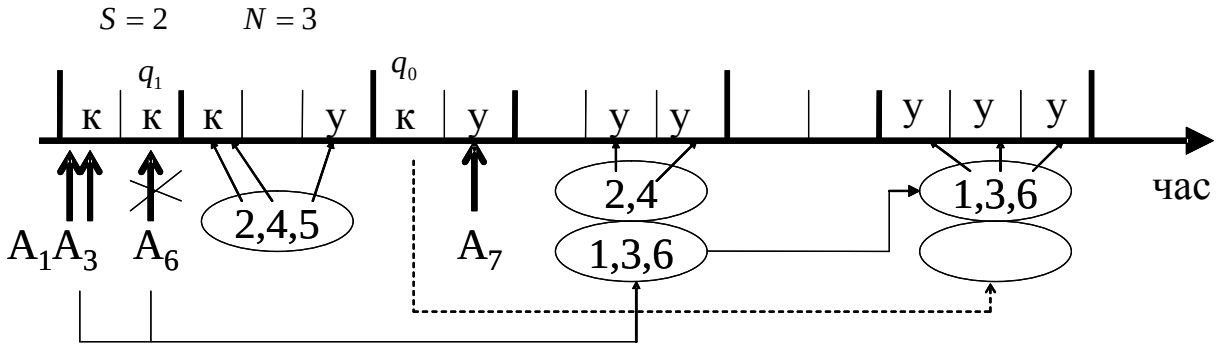


Рисунок 5.2 – Приклад функціонування алгоритму FS–ALOHA

Для обчислення швидкості FS–ALOHA функціонування алгоритму можна описати в термінах теорії систем масового обслуговування як черга FIFO GI/GI/1. Умова стійкості даної системи:

$$\Lambda(\lambda, q_0, q_1) < \mu(\lambda, q_0, q_1). \qquad 5.3$$

де $\Lambda(\lambda, q_0, q_1)$ – це середня кількість КП, що утворяться протягом одного кадру. А інтенсивність обслуговування $\mu(\lambda, q_0, q_1)$ може бути обчислена як середня кількість КП, які обслуговуються за один кадр, за умови, що в системі присутня хоча б одне КП. У магістерській роботі умова стійкості (5.2) приймає наступний вид:

$$T(\lambda, q_0, q_1) < 1, \qquad 5.4$$

де $T(\lambda, q_0, q_1) \triangleq \sum_j T_j P_{arr}(j, \lambda, S, q_0, q_1)$. Величина T_j – це математичне очікування числа кадрів, необхідних для обслуговування одного КП, що містить j запитів. Імовірність $P_{arr}(j, \lambda, S, q_0, q_1)$ – це ймовірність того, що в каналі з пуассонівським вхідним потоком інтенсивності λ запитів розраховуючи на кадр і з помилковими конфліктами, обумовленими ймовірностями q_0, q_1, на S слотах доступу утвориться КП, що містить j запитів.

Гранична інтенсивність $\lambda_{\max}$, при якій система стійка, може бути визначена як максимальна інтенсивність λ, при якій виконується нерівність (3.5). Тоді швидкість алгоритму FS–ALOHA обчислюється так: $R = \lambda_{\max} / L$.

З робіт Блонді треба, що алгоритм FS–ALOHA має максимальну швидкість у безшумному каналі при параметрах $S = 1$ і $N = 2$. У магістерській роботі показано, що це справедливо й у каналі із шумом. Саме для параметрів $S = 1$ і $N = 2$ обчислене критичне значення q_c ймовірності помилкового конфлікту, при якому швидкість FS–ALOHA дорівнює нулю, тобто при однаковій імовірності помилкових конфліктів $q = q_0 = q_1$ швидкість дорівнює нулю, якщо виконується наступна нерівність:

$$q \geq q_c = \frac{3 - \sqrt{5}}{2}. \qquad 5.5$$

Більше складний підхід до опису функціонування алгоритму FS–ALOHA дозволяє знайти розподіл ймовірностей для затримки запиту.

Процес функціонування алгоритму FS–ALOHA описується багатомірним Марківським процесом, що складається із трьох компонентів:

$$(G, r, \vec{b}), \qquad 5.6$$

де G – кількість КП, r – кількість запитів у що обслуговується КП. Третій компонент являє собою вектор $\vec{b} = (b_1, b_2 \ldots b_G)$, де b_i – кількість запитів в i–тім КП.

У магістерській роботі доведено, що якщо багатомірний марковський процес $(G, r, \vec{b})$ описати двовимірним процесом (G, r), то для стаціонарного режиму двовимірний процес теж буде Марківським. Метод розрахунку розподілу ймовірностей для затримки запиту заснований на аналізі саме двовимірної марківського ланцюга. При цьому розраховується стаціонарний розподіл ймовірностей для станів системи за допомогою матриці перехідних ймовірностей марківського ланцюга.

5.4 Алгоритми ефективні для передачі запитів при великому розмірі конкурентного інтервалу, розроблені на базі FS–ALOHA.

Представлені алгоритми, які ефективні для передачі запитів при великому розмірі конкурентного інтервалу. Алгоритми розроблені на базі FS–ALOHA. З робіт Блонди відомо, що при збільшенні розміру конкурентного інтервалу ефективність алгоритму FS–ALOHA щодо затримки різко знижується. У розділі 3 представлені алгоритми, що вирішують проблему зниження ефективності. Першим розглядається алгоритм, функціонування якого спрощено можна описати як паралельну роботу декількох алгоритмів FS–ALOHA з одним слотом доступу й двома слотами дозволу конфліктів. У цьому алгоритмі кількість слотів дозволу конфліктів N_t залежить від числа КП у черзі в кадрі з номером t. У магістерській роботі приводяться строгі правила роботи даного алгоритму, що отримав назву Multi FS–ALOHA. Приклад його функціонування зображений на малюнку 3.3 для розміру $L = 5$ конкурентного інтервалу й при максимальній кількості $N = 4$ слотів дозволу конфліктів.

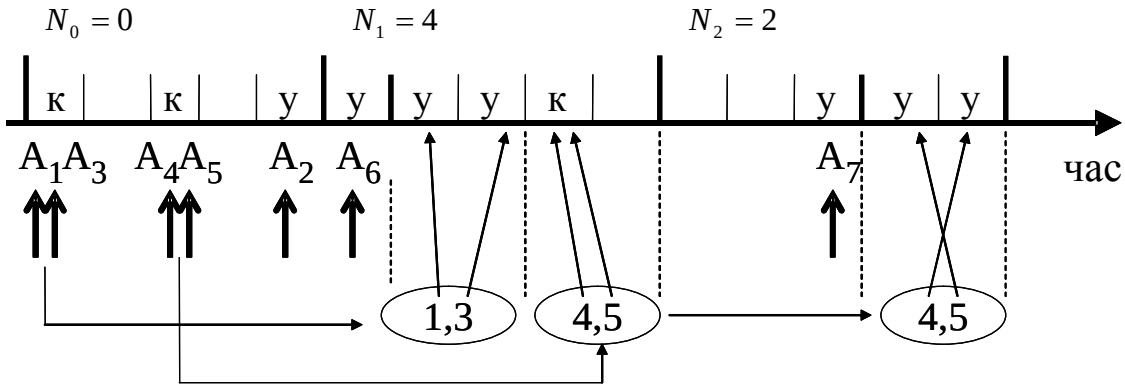


Рисунок 5.3 – Приклад функціонування алгоритму Multi FS–ALOHA

Для знаходження швидкості Multi FS–ALOHA функціонування алгоритму можна описати в термінах теорії систем масового обслуговування як черга FIFO GI/GI/(N / 2). У цьому випадку умова стійкості системи задається у вигляді нерівності

$$T(x,q_0,q_1)<\frac{N}{2S}, \qquad 5.7$$

де x – інтенсивність вхідного потоку запитів розраховуючи на слот доступу, а $T(x,q_0,q_1)$ визначається так:

$$T(x,q_0,q_1)\triangleq\sum_{j=2}^{\infty}T_j\frac{x^j}{j!}e^{-x}+T_0e^{-x}q_0+T_1xe^{-x}q_1. \qquad 5.8$$

Таким чином, швидкість алгоритму обчислюється в такий спосіб: $R=Sx_{\max}/L$, де $x_{\max}$ – це максимальна величина x, для якої виконується нерівність 5.7.

З метою знаходження оптимальних параметрів S і N, які максимізують швидкість алгоритму Multi FS–ALOHA при фіксованому розмірі L конкурентного інтервалу, визначається величина x^* – така величина x, при якій досягає максимуму наступне відношення:

$$\frac{x}{1+2T(x,q_0,q_1)}. \qquad 5.9$$

Причому величина x^* в (3.9) перебуває в припущенні, що параметри алгоритму S й N можуть бути як завгодно більшими й обрані так, щоб максимізувати (3.9).

Шукані параметри S й N для заданої величини L обчислюються за допомогою наступної системи рівнянь:

$$\begin{cases} N = 2T(x^*,q_0,q_1)S \\ L = S+N \end{cases}. \qquad 5.10$$

Розглянемо алгоритми ВМД для централізованих мереж з використанням деревоподібних АДК. У даних алгоритмах ВМД для обслуговування одного КП виділяється тільки один слот зі слотів дозволу конфліктів. Також як і в Multi FS–ALOHA, в одному кадрі може обслуговуватися відразу трохи КП. Обслуговування запитів із КП відбувається за допомогою деревоподібного АДК того або іншого виду. Алгоритми ВМД для централізованих мереж, у яких використовуються деревоподібні АДК, у магістерській роботі названі деревоподібними алгоритмами ВМД. Вид АДК є відмітною рисою одного деревоподібного алгоритму ВМД від іншого. Швидкість деревоподібних алгоритмів ВМД і їхні оптимальні параметри розраховуються тим же методом, що й в алгоритмі Multi FS–ALOHA (отримана умова стійкості аналогічне (5.7) і система рівнянь аналогічна (5.10). Результати розрахунку показані на малюнку 5.4.

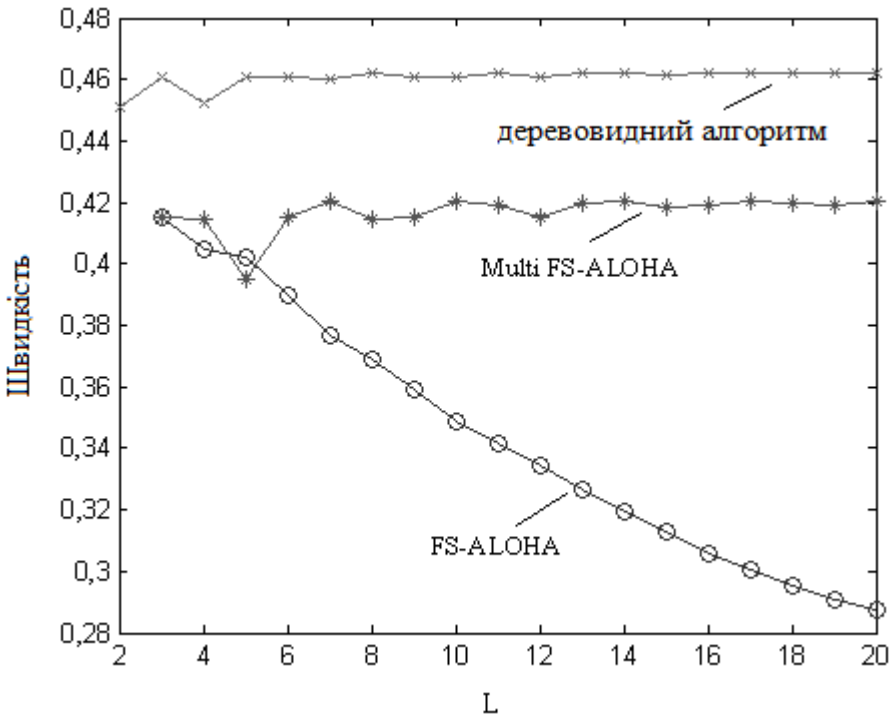


Рисунок 5.4 – Залежність швидкості Multi FS–ALOHA, FS–ALOHA і деревоподібного алгоритму від розміру L конкурентного інтервалу

При побудові залежності, зображеної на малюнку 5.4, використовувався деревоподібний модифікований алгоритм зі стеком нескінченної глибини. На цьому малюнку видно, що деревоподібний алгоритм має більшу швидкість у порівнянні з іншими алгоритмами. Але при цьому деревоподібні алгоритми мають і більшу обчислювальну складність як на стороні АС, так і на стороні ЦС.

Узагальнимо результати у двох напрямках. Перший напрямок – запропонований клас алгоритмів ВМД із чергою КП для централізованих мереж, що містить у собі як алгоритми із чергою КП, розглянуті в розділах 2 і 3, так і інші алгоритми. Другий напрямок – розглядається вхідний потік D–BMAP, часткою случаємо якого є пуассонівський вхідний потік, дослідження для якого зроблені в попередніх розділах.

Запропонований клас алгоритмів ВМД для централізованих мереж є досить широким. Він містить у собі алгоритм FS–ALOHA, а також алгоритми ВМД, які характеризуються тим, що КП утвориться із запитів попавших у

конфлікт на одному слоті, і інші алгоритми ВМД для централізованих мереж (мал. 5.5). Для конкретних умов передачі із запропонованого класу можна вибрати досить ефективний алгоритм ВМД. Наприклад, для децентралізованих мереж розроблений алгоритм дроблення, що володіє максимальною величиною швидкості $R = 0.487$ серед відомих алгоритмів ВМД. У запропонованому класі є подібний алгоритм, що у магістерській роботі умовно називається аналогом алгоритму дроблення. Для спрощення аналізу розглядається не весь клас, а деякий підклас уведеного класу. Із практичної точки зору таке звуження розгляду не істотно, оскільки в підкласі перебувають алгоритми лише що незначно уступають по швидкості алгоритму дроблення.

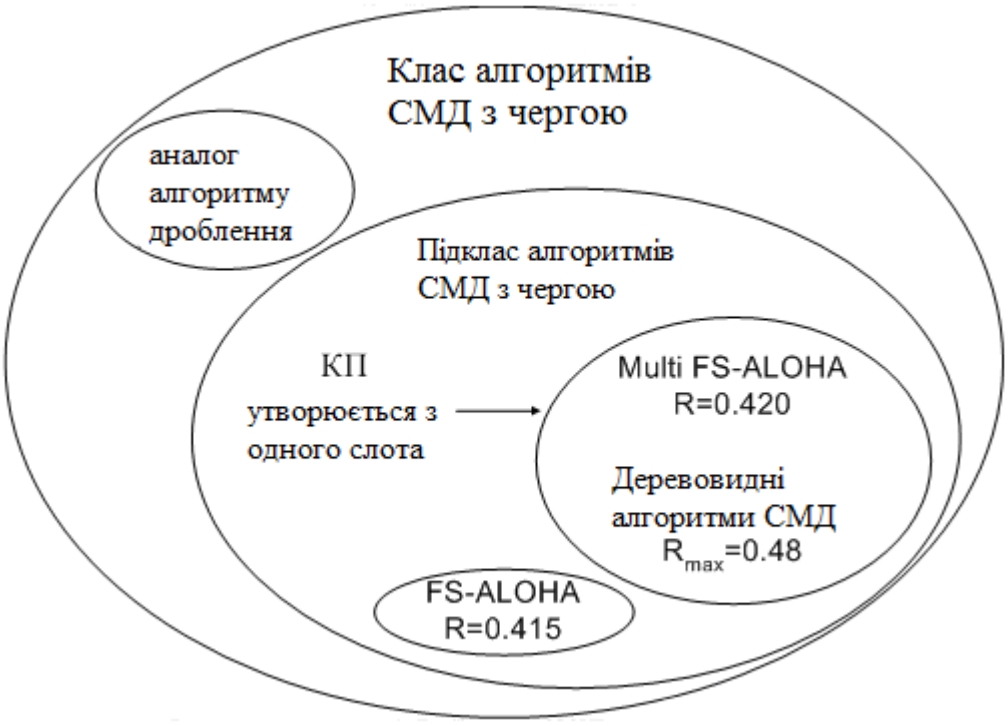


Рисунок 5.5 – Структура класу алгоритмів ВМД із чергою

У запропонованому класі алгоритмів у довільному кадрі з номером t всі L слотів конкурентного інтервалу розбиті на дві непересічні підмножини, перше з яких містить S_t слотів доступу, а друге – $N_t = L - S_t$ слотів дозволу

конфліктів. Причому слоти доступу завжди перебувають на початку конкурентного інтервалу. Параметр алгоритму $S \geq 1$ визначає мінімальне припустиме значення S_t. Тому для будь–якого кадру t вірна нерівність $1 \leq S \leq S_t \leq L$. Параметр алгоритму $N \geq 1$ визначає максимальне припустиме значення N_t. Для будь–якого кадру t виконується співвідношення $0 \leq N_t \leq N < L$. Всі слоти доступу розбиваються на групи слотів таким чином, що вони утворять *інтервали формування конфліктної підмножини*. Запити, що потрапили в конфлікт на інтервалі формування КП, формують конфліктна підмножина, що стає в чергу КП. Всі слоти дозволу конфліктів розбиваються на групи слотів таким чином, що вони утворять *інтервали обслуговування конфліктної підмножини*, у яких відбувається передача запитів з одного КП.

Умова стійкості для підкласу алгоритмів (аналогічно (3.7)) має вигляд:

$$T^a(x) < \frac{sN}{nS}, \qquad 5.11$$

де $T^a(x)$ визначається формулою

$$T^a(x) \triangleq \sum_{j=2}^{\infty} T_j^a \Pr, \qquad 5.12$$

s – розмір інтервалу формування КП, n – розмір інтервалу обслуговування КП.

У формулі (5.10) величина T_j^a – це математичне очікування числа кадрів, необхідних для обслуговування одного КП, що містить j запитів. Вираження для величин T_j^a визначаються конкретним алгоритмом a, відповідно до якого відбувається дозвіл конфлікту для абонентів із КП.

Таким чином, швидкість алгоритму обчислюється в такий спосіб: $R(S, N, s, n) = Sx_{\max} / L$, де $x_{\max}$ – це максимальна величина x, для якої виконується нерівність (3.11).

Пропонується спосіб визначення оптимальних параметрів алгоритму S й N, які максимізують швидкість алгоритму при заданому розмірі L конкурентного інтервалу. Спосіб можна використовувати для алгоритмів

ВМД, у яких величини s_t однакові для будь–якого значення S. Аналогічні умови повинні виконуватися й для n_t. Спочатку визначається величина x^* – така величина x, при якій досягає максимуму наступне відношення:

$$\frac{sx}{s+nT^a(x)}. \qquad 5.13$$

Величина x^* в (3.13) перебуває в припущенні (також як в (3.9)), що параметри алгоритму S й N можуть бути як завгодно більшими й обрані так, щоб максимізувати (3.13).

Потім обчислюються безпосередньо самі шукані параметри S й N для заданої величини L за допомогою наступної системи рівнянь:

$$\begin{cases} N = \dfrac{n}{s} S T^a(x^*) \\ L = S + N \end{cases}. \qquad 5.14$$

У магістерській роботі показано, що при знаходженні швидкості для вхідного потоку, описуваного процесом D–BMAP, також можна застосувати умова стійкості (3.11). У цьому випадку величина $T^a(x)$ визначається в такий спосіб:

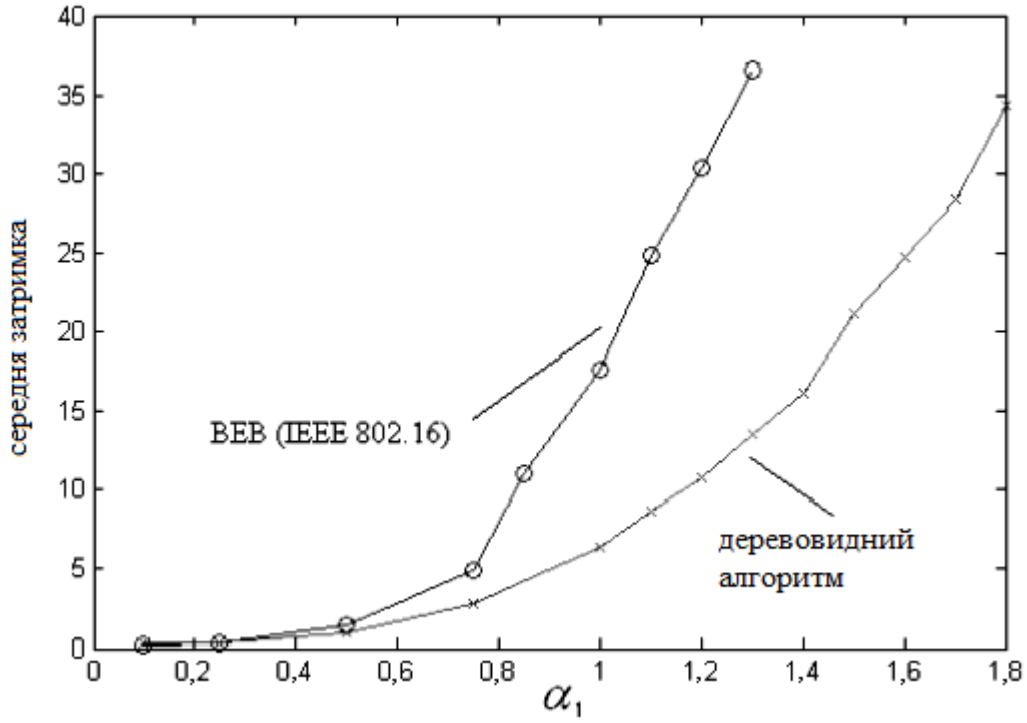
$$T^a(x) \triangleq \sum_{j=2}^{\infty} T_j^a \sum_{m=1}^{d} v_m \sum_{i=j}^{\infty} \frac{(sx_m)^i}{i!} e^{-sx_m} P_d(i-j,i,s)\ , \qquad 5.15$$

де d – кількість станів марківського ланцюга процесу D–BMAP, v_m – стаціонарна ймовірність знаходження марківського ланцюга в стані m (у якому інтенсивність вхідного потоку розраховуючи на один кадр – λ_m, а розраховуючи на слот доступу – $x_m = \lambda_m / S$). Величина x являє собою суму: $x = \sum_{m=1}^{d} v_m x_m$. Імовірність $P_d(c,i,s)$ – це ймовірність успішної передачі c запитів на інтервалі, що складається зі s слотів, за умови, що в цьому інтервалі всього передавалося випадковим образом i запитів.

За допомогою формул (5.1) і (5.11) у магістерській роботі зроблений розрахунок швидкості деревоподібного модифікованого алгоритму зі стеком нескінченної глибини для каналу зі сплесками вхідної інтенсивності.

Отримані результати свідчать про високу ефективність деревоподібного алгоритму ВМД у такому каналі. Крім того, для каналу зі сплесками вхідної інтенсивності продемонстровано, що алгоритми із запропонованого класу дозволяють досягати кращих характеристик по затримці, чим алгоритм ВЕВ, використовуваний у стандарті IEEE 802.16. Перевага показана на прикладі процесу D–BMAP, у якому є два стани марківського ланцюга – стан сплеску й нормальний стан. Даний процес задається матрицею перехідних ймовірностей, інтенсивністю λ_1 пуассонівського вхідного потоку в першому стані (стан сплеску) марківського ланцюга й інтенсивністю λ_2 пуассонівського вхідного потоку в другому стані (нормальний стан) марківського ланцюга. Інтенсивності λ_1 й λ_2 визначені розраховуючи на кадр. Якщо ланцюг перебуває в стані i, то інтенсивність пуассонівського вхідного потоку буде $\alpha_i = \lambda_i / L$ запитів розраховуючи на один слот. Оцінки середньої затримки, знайдені за допомогою імітаційного моделювання, зображені на малюнку 3.6.

Результати, показані на малюнку 5.6, демонструють залежність середньої затримки від величини α_1 при фіксованій величині $\alpha_2 = 0{,}1$. Вектор стаціонарних ймовірностей для марківського ланцюга являє собою наступний вектор: $\vec{v} = (0{,}1 \;\; 0{,}9)$. На малюнку 5.6 показано, що при сплесках інтенсивності вхідного потоку деревоподібний алгоритм ВМД має краще показники середньої затримки, чим алгоритм ВЕВ. Ефективність деревоподібних алгоритмів у каналі зі сплесками, що підтверджується зокрема даним прикладом, має велике значення на практиці, де в довільний момент часу в абонентів може виникнути велика кількість нових запитів.



Малюнок 5.6 – Залежність середньої затримки (виміряється в кадрах) від інтенсивності α_1 вхідного потоку в стані сплеску для деревоподібного модифікованого алгоритму зі стеком нескінченної глибини й алгоритму BEB

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

6.1. Вимоги до повітря робочої зони у виробничих приміщеннях

Людина відчуває себе добре і є працездатною, якщо температура навколишнього повітря 12...22°С, відносна вологість 40...60%, а рух повітря 0,1...0,2 м/с. Атмосферний тиск також має вплив на організм людини.

Процес дії метеорологічних умов на організм людини тісно пов'язаний з процесами терморегуляції організму. Людина втрачає тепло унаслідок витрати енергії на виконувану роботу, різниці між абсолютною і максимальною вологістю повітря і фактичною швидкістю переміщення повітря на робочому місці. Знаходячись в стані спокою, людина віддає тепло в середньому 10080...11340 Дж/доб (2400...2700 ккал/доб),а у робітників, зайнятих фізичною працею, віддача тепла складає 25200 Дж/доб (6000 ккал/доб). Фізична робота при високих температурах в поєднанні з високою волоістю може привести до теплового удару. При низьких температурах організм людини переохолоджується.

По кількості витраченої енергії роботи ділять на: легкі фізичні, середньої тяжкості і важкі фізичні.

ГОСТ 12.1.005—76 ССБТ. Повітря робочої зони. Загальні санітарно-гігієнічні вимоги» встановлює оптимальні і допустимі величини температури, відносної вологості і швидкості руху повітря для робочої зони виробничих приміщень. Норми складені з урахуванням надлишків явного тепла, тяжкості виконуваної роботи і сезонів року .

Оптимальні мікрокліматичні умови створюють відчуття теплового комфорту і передумови для високого рівня працездатності.

Допустимі мікрокліматичні умови — це поєднання параметрів мікроклімату, які при тривалій і систематичній дії на людину можуть викликати скороминущі і такі що швидко нормалізуються зміни

функціонального і теплового стану організму, що не виходять за межі фізіологічних пристосувальних можливостей. При цьому стан здоров'я не порушується, але можуть спостерігатися дискомфортні тепловідчуття, погіршення самопочуття і пониження працездатності.

Якщо середня температура зовнішнього повітря в 13 год найжаркішого місяця перевищує 25°С (23°С — для важких робіт), в теплий період року можна підвищувати допустиму температуру повітря у виробничих приміщеннях на постійних робочих місцях при збереженні відповідних значень відносної вогкості повітря на 3°С, але не вище 31°С в приміщеннях з незначними надлишками явного тепла і на 5°, але не вище 33°С в приміщеннях із значними надлишками явного тепла.

В холодний і перехідний періоди року у виробничих приміщеннях, в яких виконують роботи середньої тяжкості і важкі, а також при застосуванні системи опалювання і вентиляції із зосередженою подачею повітря допускається збільшувати швидкість руху повітря до 0,7 м/с на постійних робочих місцях при одночасному підвищенні температури повітря на 2°С

Стандартом передбачено, що в опалювальних виробничих приміщеннях, а також в приміщеннях із значними надлишками явного тепла, де на кожного працюючого відводиться від 50 до 100 м² площі підлоги, в холодний і перехідний періоди року допускається пониження температури повітря зовні постійних робочих місць до 12°С при легких роботах, до 10°С при роботах середньої тяжкості і до 8°С при важких роботах. В приміщеннях з площею підлоги на одного працюючого більше 100 м² температура, відносна вологість повітря, повинні бути забезпечені тільки на постійних робочих місцях.

6.2 Основні методи та засоби нормалізації повітря робочої зони

Для створення метеорологічних умов у виробничих приміщеннях, відповідних санітарним нормам, необхідно максимально механізувати

трудомісткі процеси, ретельно герметизувати устаткування, що є джерелом підвищеного тепло-, вологовиділення. Санітарно-гігієнічні умови повітряного середовища у виробничих приміщеннях можна забезпечити також за допомогою природної, механічної і змішаної вентиляції.

В природних системах вентиляції повітря переміщається в результаті різниці тиску зовнішнього і внутрішнього повітря або під дією вітру. В механічних системах вентиляції повітря переміщається за допомогою вентиляторів.

За принципом розміщення приточних і витяжних пристроїв вентиляцію підрозділяють на загальну і місцеву. При загальній вентиляції повітрообмін здійснюється шляхом подачі і видалення повітря зі всього приміщення. Місцеву вентиляцію звичайно влаштовують у виробничих приміщеннях, де головні джерела виділення шкідливих речовин зосереджені в певних місцях. Вона призначена також для видалення надмірної вологи і тепла, створення розрідження в захисних кожухах машин. До місцевої вентиляції відносяться витяжні шафи в лабораторіях, аспіраційне відсмоктування пилу у скидаючих коробках, візках, насипних лотках, стрічкових транспортерах, приймальних столах гвинтових і похилих спусках в складах, приймальних пристроях, столах для сортування, очищення і ремонту м'якої тари.

Вентиляція може бути :

- Приточна вентиляція здійснюється подачею свіжого повітря в приміщення.
- Витяжна — видаленням забрудненого повітря з приміщення
- Приточно-витяжна — одночасною подачею свіжого повітря в приміщення і видаленням з нього забрудненого.

Аспіраційні мережі на хлібоприймальних і зернопереробних підприємствах працюють за схемою витяжної вентиляції. Повітря з приміщення відсмоктується через устаткування і транспортні механізми, очищається в пилевідділювачі і виводиться в атмосферу. Видалене з

приміщень повітря заміщається організованим і неорганізованим притоком зовнішнього повітря. Організований повітрообмін в приміщеннях регулюють, відкриваючи кватирки, віконні отвори і т. і. При неорганізованому притоці обмін повітря відбувається через випадкові отвори (нещільність стін, дверей, стель).

В холодну пору року великий обмін повітря в приміщеннях знижує температуру, виникають протяги, що погіршує умови праці і викликає простудні захворювання. Тому доступ холодного повітря в приміщення обмежують. Створюваний при цьому у виробничих приміщеннях вакуум впливає на самопочуття, здоров'я і працездатність людей. Нерідко кратність повітрообміну у виробничих приміщеннях значно перевищує санітарні норми (в 1-2 рази на годину). Переміщувані потоки повітря несуть за собою пил, який осідає на устаткуванні, світильниках, будівельних конструкціях, утворюючи вибухонебезпечну концентрацію. Вакуум утрудняє знепилювання устаткування, знижує корисну подачу повітря вентиляторами. Для усунення вакууму у виробничих приміщеннях застосовують аспіраційні мережі з рециркуляцією (зворотним поверненням) знепиленого повітря, яке очищають і зволожують до встановлених норм.

Рециркуляційні апарати повинні бути надійними перепонами на шляху вогню і не допускати концентрації пилу в рециркуляційному повітрі вище 1 мг/м³. Для рециркуляції повітря і опалювання у виробничих приміщеннях застосовують калорифери і кондиціонери. Продуктивність кондиціонерів типу КТ по повітрі— 10, 20, 40, 60 тис. м³/год.

Швидкість руху повітряного потоку, що подається з систем опалювання і рециркуляції, під час вступу до робочої зони не повинна перевищувати в холодний і перехідний періоди року 0,5 м/с.

Відповідно до галузевих правил техніки безпеки виробничі приміщення мукомельних заводів і цехів, приміщення диспетчерської, кімнати начальників цеху, їдальні, червоні кути, санвузли (за наявності

каналізації), приміщення для обігріву працюючих на відкритому повітрі опалюють. Для цього застосовують системи повітряного, центрального водяного або парового опалювання.

Опалювальні прилади повинні мати гладку поверхню, їх встановлюють на висоті, доступній для прибирання пилу. Прилади опалювання не можна закривати і загороджувати устаткуванням, матеріалами і т.п. Температура нагрітих поверхонь устаткування і огорож на робочих місцях не повинна перевищувати 45°С.

В неопалювальних виробничих приміщеннях і складах влаштовують спеціальні кабіни для обігріву. Для захисту виробничих приміщень від проникаючого в них холодного повітря при відкритті дверей застосовують повітряно-теплові завіси.

6.3 Природне освітлення та основні вимоги до його організації

Вимоги до освітленості виробничих приміщень.

Правильно організоване освітлення створює достатню і рівномірну освітленість робочих місць, підвищує продуктивність праці і якість роботи, зберігає зір працюючих, зменшує травматизм, сприятливо діє на нервову систему і організм людини.

Природне освітлення надає сприятливу дію на організм людини і повинне бути використаний максимально. Воно здійснюється через бічні світлові отвори (вікна)—бокове освітлення і через верхні світлові отвори (ліхтарі) — верхнє освітлення.

Для характеристики інтенсивності денного освітлення прийнятий коефіцієнт природної освітленості. коефіцієнт є відношенням природної освітленості усередині приміщення (Ев) до одночасного значення зовнішньої горизонтальної освітленості (Ен), створюваної світлом повністю відкритого небосхилу. Його визначають за формулою

$$l=(Ев)/ (Ен)\cdot 100$$

В Правилах техніки безпеки і виробничої санітарії на підприємствах, в організаціях і установах приводяться норми коефіцієнта природної освітленості .

Якщо будівля розташована на південь від 45° північної широти, коефіцієнт природної освітленості множать на поправочний коефіцієнт 0,75.

Якщо приміщення освітлюється тільки бічним світлом, встановлюють мінімальне значення коефіцієнта (e_{min}) в точках, самих віддалених від вікон, а для приміщення з верхнім або комбінованим освітленням—його середнє значення ($e_{ср}$) , яке в 3...4 рази більше e_{min}.

Відповідно до санітарних норм СН 245-71 всі виробничі приміщення, розраховані на тривале перебування людей, повинні мати природне освітлення. Скло світлових отворів виробничих і допоміжних приміщень очищають в терміни, встановлені адміністрацією підприємства, але не рідше 2 раз на рік. Світлові отвори не можна захаращувати устаткуванням. Світле забарвлення інтер'єру покращує якість освітлення, оскільки збільшується кількість відобитого світла, що дозволяє підвищити рівень освітленості.

6.4 Небезпечні та шкідливі фактори виробництва

В процесі праці на людину короткочасно або тривало впливають різноманітні несприятливі фактори, які можуть привести до захворювання і втрати працездатності. Небезпечний виробничий фактор — це фактор, дія якого на працюючого приводить до травми. Шкідливий виробничий фактор — це чинник, дія якого на працюючого приводить до захворювання.

Небезпечні і шкідливі виробничі чинники підрозділяють на чотири групи: фізичні, хімічні, біологічні і психофізіологічні.

До фізичних чинників відносять: машини і механізми, незахищені рухомі елементи виробничого устаткування, вироби, заготівки, матеріали, що пересуваються, що рухаються; підвищену запорошеність і загазованість повітря робочої зони; підвищену або знижену температуру повітря робочої

зони; підвищений рівень шуму і вібрації; підвищену або знижену вогкість повітря; підвищену або знижену рухливість повітря; відсутність або недолік природного світла; недостатню освітленість робочої зони.

Хімічні фактори по характеру дії на організм людини ділять на загальнотоксичні, дратівливі, канцерогенні, мутагенні, впливаючі на репродуктивну функцію. По шляху проникнення в організм людини хімічні чинники підрозділяють на діючі через дихальні шляхи, травну систему і шкірний покрив.

До групи біологічних факторів відносять об'єкти, дія яких на працівників може викликати травми або захворювання — мікроорганізми (бактерії, віруси тощо) і макроорганізми (рослини і тварини).

До психофізіологічних фактори відносять фізичні (статичні, динамічні, гіподинамічні) і нервово-психічні перевантаження (розумове перенапруження, емоційні перевантаження, монотонність праці, перенапруження аналізаторів).

Санітарні норми і державні стандарти передбачають гранично допустимі концентрації шкідливих речовин в повітрі робочої зони. По ступеню дії на організм людини шкідливі речовини підрозділяють на чотири класи: надзвичайно небезпечні, високонебезпечні, помірно небезпечні, малонебезпечні. Одним з чинників, що характеризують клас небезпеки, є гранично допустима концентрація шкідливих речовин в повітрі робочої зони: для 1-го класу менше 0,1 мг/м³, для 2-го —від 0,1 до 1, для 3-го —від 1,1 до 10, для 4-го — понад 10 мг/м³.

6.5 Безпека у надзвичайних ситуаціях

6.5.1 Класифікація надзвичайних ситуацій

Надзвичайні ситуації (НС) прийнято класифікувати за сферою виникнення, характером протікання, масштабом і ступенем завданого збитку, а також за відомчою приналежністю. За сферою виникнення надзвичайні ситуації поділяються на техногенні, природні, біолого- соціальні і соціальні, екологічні і надзвичайні ситуації військового характеру (рис. 6.1).

Техногенні надзвичайні ситуації

Можуть виникають на основі подій техногенного характеру внаслідок конструктивних недоліків об'єкту (споруди, комплексу, системи, агрегату тощо), зношування устаткування, низької кваліфікації персоналу, порушення техніки безпеки в ході експлуатації об'єкту і так далі. НС техногенного характеру можуть протікати із забрудненням довкілля або без нього.

Забруднення довкілля може відбуватися при аваріях на промислових підприємствах з викидом радіоактивних, хімічно небезпечних, біологічно небезпечних речовин. До аварій з викидом або загрозою викиду радіоактивних речовин (РВ) відносяться аварії, що відбуваються на атомних станціях, ядерних науково-дослідних реакторах, підприємствах ядерно-паливного циклу, атомних судах, при падінні літальних апаратів з ядерними енергетичними установками на борту, а також на підприємствах ядерно-збройного комплексу. В результаті таких аварій може виникнути сильне радіоактивне забруднення місцевості або акваторії.

До НС техногенного характеру відноситься також електро- магнітне забруднення довкілля при функціонуванні техногенних джерел електромагнітного випромінювання (ЕМІ), що створюють електромагнітні поля підвищеної інтенсивності.

До НС без забруднення довкілля відносять аварії, що супроводжуються вибухами, пожежами, руйнуванням будівель (споруд), порушенням систем життєзабезпечення, руйнуванням гідротехнічних систем, порушенням транспортних комунікацій і тому подібне.

Надзвичайні ситуації природного характеру

Виникають як правило, в результаті катастроф стихійних лих та інших природних явищ, викликаних як зовнішніми, так і внутрішніми причинами дії різних сил природи на біосферу. Зовнішні дії обумовлені впливом далекого космосу (Галактика, Сонячна система), накладенням процесів ближнього космосу (магнітосфери, атмосфери), а також процесами, що виникають безпосередньо на поверхні Землі.

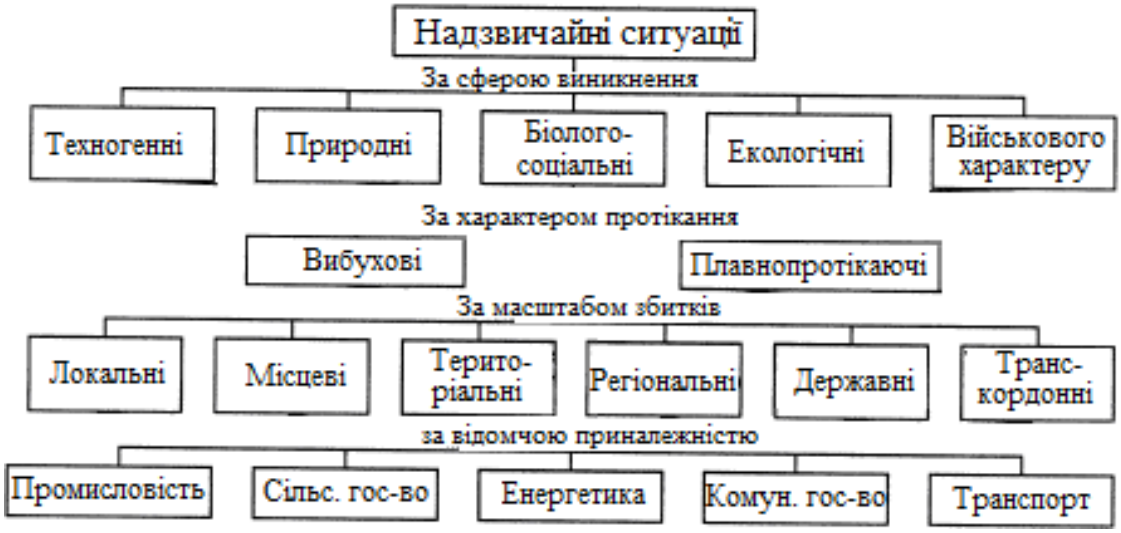


Рисунок 6.1 – Класифікація надзвичайних ситуацій

Внутрішні процеси Землі пов'язані з диференціацією речовини і розшаруванням її за фізико-механічними властивостями, вони супроводжуються такими явищами, як інверсія магнітного поля, магматична і тектонічна активність, рух літосферних плит, вулканізм, сейсмічність тощо. Усі ці процеси з різною періодичністю в часі діють на біосферу і сприяють виникненню катастроф. Статистичний аналіз показує, що з природних явищ, з точки зору нанесення збитку і ураження людей, на першому місці стоять

повені. Далі йдуть землетруси, виверження вулканів, кліматичні зміни, погодні дії. При цьому існує небезпечна тенденція збільшення числа природних катастроф, зараз їх відбувається в п'ять разів більше, ніж в 60-х роках, а економічний збиток від них зріс більш, ніж у 8 разів.

Крім того, швидкий розвиток продуктивних сил, безконтрольне освоєння вільних територій, праця в районах з кліматичними умовами, де зберігається постійна небезпека виникнення природних катаклізмів збільшують ступінь ризику і масштаби втрат і збитку для населення і економіки. Нерідко природні явища стають прямою або непрямою причиною аварій і катастроф техногенного характеру.

Природні НС поділяються за підгрупами відповідно до небезпечності, і типу стихії, що їх викликає, на: геофізичні, геологічні, метео- і агрометеорологічні, морські гідрогеологічені, гідрологічно небезпечні явища і природні пожежі.

Кожна група стихійних лих класифікується по характеру явищ, які визначають особливості дії властивих їм вражаючих (руйнівних) чинників на населення, природу і об'єкти економіки.

До стихійних лих, пов'язаних з геофізично небезпечними явищами, відносяться землетруси, виверження вулканів і тому подібне. До геологічних небезпечних явищ відносяться зсуви, селі, осипи, лавини. Такі природні явища, як селеві потоки і лавини

найчастіше виникають в гірських районах.

Стихійні лиха, пов'язані з метеорологічними і агрометео- рологічними небезпечними явищами підрозділяються на лиха, що викликаються вітром (бурі, урагани, шквали і смерчі), сильним дощем (при кількості опадів 50 мм протягом 12 год і менше), великим градом (при діаметрі градин 20 мм і більше), сильними снігопадами (при кількості опадів 20 мм і більше за 12 год і менше), сильними завірюхами (при швидкості вітру 15 м/с); сильною ожеледдю, заморозками і суховіями.

Стихійні лиха, пов'язані з морськими гідрологічними небезпечними явищами, підрозділяються на лиха, що викликаються сильним хвилюванням на морях (при висоті хвиль, особливо небезпечних для мореплавання і берегових споруд), цунамі (при затопленні населених пунктів і об'єктів економіки) тощо. Гідрологічні небезпечні явища можуть бути викликані високими рівнями води, повенями і низьким рівнем води на судноплавних ріках, селями, що утворилися при прориві загат, завальних і морених озер із загрозою населеним пунктам та іншим важливим об’єктам.

Природні пожежі, в першу чергу лісові і торфяні, є найпоширенішими лихами для населення, економіки і природного середовища.

До біолого-соціальних НС відносяться інфекційні захворювання людей, сільськогосподарських тварин і ураження сільськогосподарських рослин різного масштабу. До соціальних НС відносяться: падіння репродукції населення, масові заворушення серед населення, тероризм в різних сферах його прояву, негативна обстановка в творчих і виробничих колективах тощо.

До надзвичайних ситуацій екологічного характеру відносять зміни стану атмосфери, суші, гідросфери і біосферу в цілому. НС екологічного характеру найчастіше виникають в результаті несприятливого впливу техногенної діяльності людини на довкілля, хоча часто їх причиною можуть бути стихійні явища, а також комплексна дія техногенних і природних чинників, В результаті порушень стану атмосфери можлива зміна клімату, виникнення гострого кисневого голодування у великих містах, утворення великих зон "кислотних дощів", руйнування озонового шару над населеними територіями та інші подібні явища. Несприятливі зміни в стані суші можуть призводити до деградації грунтів, втрати корисних площ і виснаження невідновлюваних запасів корисних копалини.

6.5.2 Безпека у надзвичайних ситуаціях на робочому місці

При роботі в кабінеті можуть виникнути надзвичайні ситуації наступних класів:

- умисні / ненавмисні;
- техногенні (вибухи, пожежі, обвалення приміщень, аварії на системах життєзабезпечення / природні - пов'язані з проявом стихійних сил природи);
- екологічні (забруднення біосфери, руйнування озонового шару, кислотні дощі / антропогенні - є наслідком помилкових дій людей).
- біологічні (різні епідемії, епізоотії); комбіновані.

Основним джерелом надзвичайних небезпек при розробці програмного продукту є виникнення пожежі, виникнення інших видів НС малоймовірно.

Забезпечення пожежної безпеки установ досягається, перш за все, встановленням жорсткого протипожежного режиму і навчанням обслуговуючого персоналу заходам пожежної безпеки і діям під час пожежі.

Територія установи, а також ділянки, прилеглі до нього, повинні своєчасно очищуватися від горючих відходів, сміття, які слід збирати на спеціально виділених майданчиках у контейнери або ящики, а потім вивозити на звалище. Необхідно контролювати стан доріг, проїздів, під'їздів і проходів до будівель, стежити за тим, щоб вони нічим не захаращувати, а в зимовий час регулярно очищалися від снігу і льоду. У будівлях, що належать до об'єктів з масовим перебуванням людей, особлива увага повинна приділятися утримання шляхів евакуації. Кожна будівля повинна мати не менше двох евакуаційних виходів, всі двері евакуаційних виходів повинні вільно відкриватися в бік виходу з приміщень.

На випадок відключення електроенергії, у обслуговуючого персоналу повинні бути електричні ліхтарі.

На кожному поверсі будівлі, на видному місці повинен бути вивішений план евакуації (рис.6.2) з поверху (будівлі).

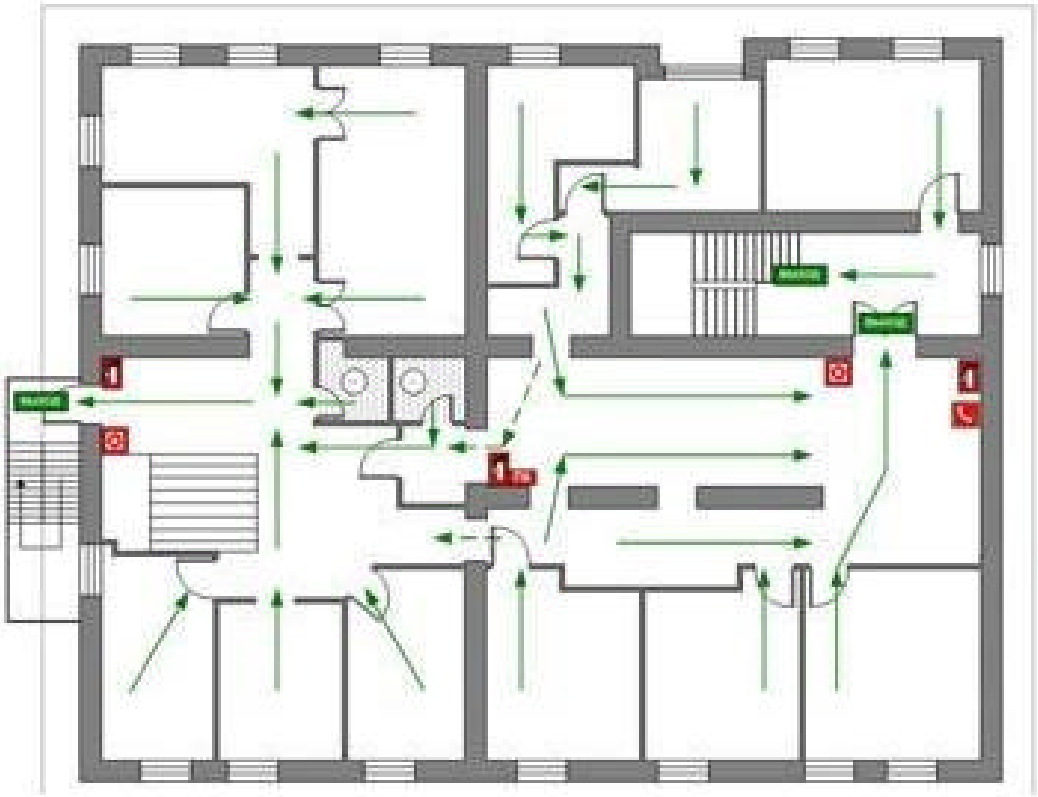


Рисунок 6.2 – План евакуації

Необхідно проводити такі пожежно-профілактичні заходи:

організаційні:

- протипожежний інструктаж обслуговуючого персоналу;
- навчання персоналу правилам техніки безпеки;

експлуатаційні:

- дотримання експлуатаційних норм обладнання;
- забезпечення вільного підходу до обладнання;
- утримання в справності ізоляції струмоведучих провідників;

технічні:

- дотримання протипожежних заходів при влаштуванні електропроводок, обладнання, систем опалення, вентиляції та освітлення;
- профілактичний огляд, ремонт і випробування обладнання.

У разі виникнення пожежі співробітники повинні вживати таких заходів:

- повідомити про пожежу в пожежну охорону, задіяти систему оповіщення;
- задіяти план евакуації (відкрити запасні двері і включити світлові таблички евакуаційних шляхів);
- вивести людей в безпечне місце відповідно до плану евакуації;
- перевірити поіменно, чи всі евакуйовані;
- приступити до гасіння пожежі первинними засобами;
- зустріти пожежні підрозділи і повідомити, де могли залишитися люди, як туди можна підійти;
- вжити заходів до евакуації майна.

Для гасіння пожеж слід застосовувати вуглекислотні та порошкові вогнегасники, які мають високу швидкість гасіння, великим часом дії, можливістю гасіння електроустановок, високою ефективністю боротьби з вогнем. Воду дозволено застосовувати тільки в допоміжних приміщеннях.

ВИСНОВОК

Завданням рівня передачі даних є перетворення неопрацьованого потоку бітів, що надходить із фізичного рівня, у потік кадрів, що може використовувати мережевий рівень. У даній магістерській роботі були розглянуті різні методи кадрування, включаючи підрахунок символів, символьне й бітове заповнення. Протоколи рівня передачі даних можуть мати можливості контролю помилок, що здійснюється при повторній передачі загублених та зіпсованих кадрів.

Також у даній роботі розглянуті протоколи множинного доступу, такі як сімейства протоколів ALOHA і CSMA. Дано описи роботи протоколів і оцінена їхня ефективність. Наведено порівняльних графіків ККД протоколів.

Були розглянуті приклади конкретних протоколів (Ethernet, Token Ring, FDDI).

В результаті проведених досліджень:

1. Досліджено базовий алгоритм FS–ALOHA із чергою для каналу із шумом. Отримано аналітичні вираження для чисельного розрахунку швидкості FS–ALOHA. Виявлено оптимальні щодо швидкості параметри алгоритму й доведено, що при досягненні рівнем шуму певної величини, швидкість алгоритму стане рівної нулю. Розроблено метод розрахунку розподілу ймовірностей для затримки запиту. Показано перевагу в цілому алгоритму FS–ALOHA перед BEB, що використовується в стандарті IEEE 802.16.

2. Запропоновано алгоритм, що є модифікацією алгоритму FS–ALOHA – Multi FS–ALOHA. На відміну від FS–ALOHA, в алгоритмі Multi FS–ALOHA не знижується швидкість при збільшенні розміру конкурентного інтервалу. Отримано аналітичні вираження для чисельного розрахунку швидкості алгоритму Multi FS–ALOHA у каналі із шумом. Зазначено спосіб визначення

параметрів алгоритму, при яких його швидкість максимальна. Показано, що алгоритм FS–ALOHA більше підданий впливу шумів у порівнянні з Multi FS–ALOHA.

3. Запропоновано деревоподібні алгоритми для централізованих мереж. Алгоритми є аналогами високошвидкісних деревоподібних алгоритмів з віконним доступом для децентралізованих мереж. Деревоподібні алгоритми багато в чому схожі з Multi FS–ALOHA, але завдяки використанню деревоподібного АДК мають більше високу швидкість. Але при цьому Multi FS–ALOHA має меншу обчислювальну складність. Отримано аналітичні вираження для чисельного розрахунку швидкості деревоподібних алгоритмів і визначення їхніх оптимальних параметрів. Ефективність використання таких алгоритмів продемонстрована на прикладі модифікованого алгоритму зі стеком нескінченної глибини. Алгоритм показав високі результати, як щодо швидкості, так і щодо середньої затримки. Особливо ефективний алгоритм у каналі зі сплесками вхідної інтенсивності.

4. Запропоновано клас алгоритмів ВМД із чергою для конкурентного каналу централізованих мереж. Даний клас містить широкий спектр алгоритмів від базового алгоритму із чергою (FS–ALOHA) до аналога алгоритму дроблення для централізованих мереж. Розроблено метод обчислення швидкості для алгоритмів ВМД, що входять у підклас алгоритмів уведеного класу. Розроблено метод визначення оптимальних щодо швидкості параметрів алгоритму з підкласу алгоритмів ВМД. Отримано метод обчислення швидкості алгоритму з підкласу алгоритмів ВМД для різних видів вхідних потоків, описуваних марківського ланцюгом (D–BMAP).

5. Розроблено комплекс програм імітаційного моделювання й чисельного розрахунку швидкості для запропонованих алгоритмів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Ziv J. and Lempel A A universal algorithm for sequential data compression IEEE Transactions on Information Theory. Vol. IT–23, № 3, May 1977, pp. 337–343
2. Ziv J. and Lempel A Compression of individual sequences via variable rate coding IEEE Transactions on Information Theory. Vol. IT–24. № 5, September 1978, pp. 530–535
3. Burrows M. and Wheeler D.J A block–sorting Lossless Data Compression Algorithm Digital Systems Research Center. SRC report 124. May 10, 1994
4. Bently J.L., Sleator D.D., Tarjan R.E., and Wei V.K A locally adaptive data compression algorithm Communications of the ACM, Vol. 29, № 4, April 1986, pp. 320–330
5. Guide to Network Resource Tools EARN Association, Sept. 15, 1993, V2.0. (ISBN 2– 910286–03–7)
6. Packets and Protocols Spider Systems, Stanwell Street, Ltd. Edinburgh, UK. EH6 5NG, 1990
7. Paul J. Fortier Handbook of LAN Technology 2–nd Edition, McGraw–Hill, 1992
8. Charles Summers, Bryant Dunetz ISDN How to get a high–speed connection to the Internet “John Wiley @ Sons, Inc.”
9. John M. Griffiths ISDN Explained, Worldwide Network and Applications Technology, 2 edition John Wiley & sons
10. Carrier Sense Multiple Access with Collision detection Access Method and Physical Layer Specification Published by IEEE 802.3–1985. WileyInterscience, John & Sons, Inc

11. Проектування мікропроцесорних систем керування: навчальний посібник/ І.Р. Козбур, П.О. Марущак, В.Р. Медвідь, В.Б. Савків, В.П. Пісьціо.–Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2022.–324с.
12. Я.І. Проць, В.Б. Савків,О.К. Шкодзінський, О.Л. Ляшук. Автоматизація виробничих процесів. Навчальний посібник для технічних спеціальностей вищих навчальних закладів. – Тернопіль: ТНТУ ім. І.Пулюя, 2011. – 344с.
13. Основи наукових досліджень і теорія експерименту : Навчальний посібник / укл. Ю. Б. Капаціла, П. О. Марущак, В. Б. Савків, О. П. Шовкун. Тернопіль : ФОП Паляниця В.А., 2023. 186 с.». http://elartu.tntu.edu.ua/handle/lib/40843.
14. Пилипець М. І. Правила заповнення основних форм технологічних документів : навч.-метод. посіб. / Уклад. Пилипець М. І., Ткаченко І. Г., Левкович М. Г., Васильків В. В., Радик Д. Л. Тернопіль : ТДТУ, 2009. 108 с. https://elartu.tntu.edu.ua/handle/lib/42995.
15. Методичний посібник для здобувачів освітнього ступеня «магістр» всіх спеціальностей денної та заочної (дистанційної) форм навчання «Безпека в надзвичайних ситуаціях» / В.С. Стручок –Тернопіль: ФОП Паляниця В. А., –156 с. https://elartu.tntu.edu.ua/handle/lib/39196.
16. Навчальний посібник «Техноекологія та цивільна безпека. Частина «Цивільна безпека»» / автор-укладач В.С. Стручок – Тернопіль: ФОП Паляниця В. А., – 156 с. http://elartu.tntu.edu.ua/handle/lib/39424
17. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 1. [навчальний посібник] (Лист МОНУ №1/11-8052 від 28.05.12р.) - Львів, "Магнолія 2006", 2013. – 256 с.
18. А.Г. Микитишин, М.М. Митник, П.Д. Стухляк, В.В. Пасічник Комп'ютерні мережі. Книга 2. [навчальний посібник] (Лист МОНУ №1/11-11650 від 16.07.12р.) - Львів, "Магнолія 2006", 2014. – 312 с.

19. Микитишин А.Г., Митник, П.Д. Стухляк. Комплексна безпека інформаційних мережевих систем: навчальний посібник – Тернопіль: Вид-во ТНТУ імені Івана Пулюя, 2016. – 256 с.
20. Микитишин А.Г., Митник М.М., Стухляк П.Д. Телекомунікаційні системи та мережі : навчальний посібник для студентів спеціальності 151 «Автоматизація та комп’ютерно-інтегровані технології» – Тернопіль: Тернопільський національний технічний університет імені Івана Пулюя, 2017 – 384 с.
21. Введення в компютерну графіку та дизайн: Навчальний посібник для студентів спеціальності 174 "Автоматизація, компютерно-інтегровані технології та робототехніка"/Укладачі: О.В. Тотосько, П.Д. Стухляк, А.Г. Микитишин, В.В. Левицький, Р.З. Золотий - Тернопіль: ФОП Паляниця В.А., 2023 - 304с. http://elartu.tntu.edu.ua/handle/lib/41166.