Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
«Київський політехнічний інститут імені Ігоря Сікорського»

СПЕЦІАЛЬНА КАФЕДРА №3

ГОЛЬ В.Д., ІРХА М.С.

СИСТЕМИ ПЕРЕДАЧІ ДАНИХ

КОНСПЕКТ ЛЕКЦІЙ

*Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
як навчальний посібник для курсантів (слухачів, студентів), які навчаються в Інституті за спеціальністю 172 «Телекомунікації та радіотехніка», галузі знань 17 «Електроніка та телекомунікації»*

Київ – 2021

УДК 621.396

Рекомендовано Вченою радою ІСЗЗІ КПІ ім. Ігоря Сікорського
(протокол № 1 від 23 вересня 2021 року)

Рецензенти: кан. техн. наук, с.н.с. *Самборський* Іван Іванович професор спеціальної кафедри № 3 Інституту Спеціального зв'язку та захисту інформації Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».
к.т.н., доцент *Правило* Валерій Володимирович, в.о. завідувача кафедри інформаційно-комунікаційних технологій та систем Інституту телекомунікаційних систем Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського».

Голь В.Д., Ірха М.С. Системи передачі даних : конспект лекцій. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 126 с.

Конспект лекцій відповідає змісту навчальної дисципліни "Системи передачі даних". Конспект лекцій містить описи 3 комплексних тем. У кінці наведено список рекомендованих навчально-методичних матеріалів.

Призначений для курсантів (слухачів, студентів) спеціальності 172 Телекомунікації та радіотехніка, галузі знань 17 Електроніка та телекомунікації, освітньо-професійної програми – Спеціальні телекомунікаційні системи.

УДК 621.396

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ДЕЗ – документальний електро зв'язок
ТМ – телематична служба
ЕОМ – електро обчислювальна машина
ВЗЗ – вирішальний зворотний зв'язок
ІЗЗ – інформаційний зворотний зв'язок
ПЗ – пропускна здатність
КК – комутаційний код
ЦСД – цифрова система даних
ЦСП – цифрова система передачі
ПД – передача даних
РП – реєструючий пристрій
ЗМ – значущі моменти
СПЕС – Система поелементної синхронізації
АФАПЧ – аналогове керування фазовою автопідстройкою частоти
ДФАПЧ – дискретне керування фазовою автопідстройкою частоти
ДАПФ – дискретне автопідстроювання фази
ФД – фазовий детектор
ПЧО – пристрої часового об’єднання
ЦР – цикловий розподільник
ФА – факсимільний апарат
КТЧ – канал тональної частоти
ФЕП – фотоелектричне перетворювання
RLE – Run Lengh Encoding – кодування довгих серій
LZW – Lempel-Ziv-Welch – алгоритм Лемпеля-Зіва-Велча
IOS – Internetwork Operating System – міжмережева операційна система корпорації Cisco
RAM – оперативний запам’ятовуючий пристрій
ROM – постійний запам’ятовуючий пристрій
NVRAM – незалежна пам’ять
IP/FW – ip firewall – міжмережевий екран
TFTP – Trivial File Transfer Protocol – спрощений протокол передачі файлів
RRQ – запит на читання файлів
WRQ – запит на запис файлів
UDP – User Datagram Protocol – протокол датаграм користувача
TCP – Transmission Control Protocol – протоко́л керува́ння переда́чею
IFS – Installable File System – API файлових систем
USB – Universal Serial Bus – універсальна послідовна шина
VLAN – Virtual Local Area Network – віртуальна лакальна комп’ютерна мережа
FHRPs – First Hop Redundancy Protocols – протокол резервування першого переходу
MAC – Media Access Control – управління доступом до посередників

ARP – Address Resolution Protocol – протокол визначення адрес
HSRP – Hot Standby Router Protocol – протокол маршрутизатора з гарячим резервуванням
VRRP – Virtual Router Redundancy Protocol – протокол резервування віртуальних маршрутизаторів
GLBP – Gateway Load Balancing Protocol – протокол балансування навантаження шлюзу
IRDP – Router Discovery Protocol протокол виявлення маршрутизатора ICMP
ICMP – Internet Control Message Protocol – міжмережевий протокол керуючих повідомлень
AVG – Active Virtual Gateway – активним віртуальним шлюзом
AVFs – Active Virtual Forwarders – активний роутер, який пропускає через себе трафік

ВСТУП

Конспект лекцій призначений для підготовки та проведення лекційних занять з навчальної дисципліни “Системи передачі даних” для курсантів (слухачів, студентів), які навчаються за спеціальністю 172 Телекомунікації та радіотехніка, галузі знань 17 – Електроніка та телекомунікації, освітньо-професійної програми – Спеціальні телекомунікаційні системи денної форми навчання.

Навчальна дисципліна належить до циклу професійної підготовки та має статус обов’язкової. Міждисциплінарні зв’язки: науковою основою навчальної дисципліни є теорія інформації, теорії передачі та прийому сигналів і передачі електромагнітної енергії по направляючих системах.

Математичною базою навчальної дисципліни є такі розділи курсу математики, як теорія множин, диференційні та інтегральні обчислення, гармонічний спектральний аналіз сигналів, теорія ймовірностей і математична статистика, теорія масового обслуговування та випадкові процеси.

Навчальна дисципліна базується на знаннях отриманих у раніше вивчених дисциплінах: теорія електричних кіл та сигналів; вища математика; телекомунікаційні системи передачі; фізика; інформатика; теорія електрозв’язку.

Навчальна дисципліна забезпечує вивчення частини розділів таких дисциплін навчального плану:

– Захист інформації в телекомунікаційних системах;
– Телекомунікаційні та інформаційні мережі;
– Системи передачі і розподілу інформації;
– Основи проектування мережевих і транспортних засобів;
– Управління потоками та сигналізація в мережах.

Після засвоєння навчальної дисципліни курсанти (слухачі, студенти) мають продемонструвати такі результати навчання:

знати:

– основні характеристики систем і мереж передачі даних та документального електрозв’язку;
– принципи організації, протоколів та умов функціонування засобів і мереж факсимільного зв’язку;
– принципи організації і побудови засобів і мереж передачі даних;
– елементи та характеристики мереж передачі даних;

вміти:

– проводити аналіз засобів і характеристик систем передачі даних та інших видів документального електрозв’язку;
– здійснювати кількісну оцінку основних технічних характеристик і параметрів каналів передачі даних та інших видів документального електрозв’язку;

– аналізувати режими роботи та схеми трактів передачі та прийому даних;

– виконувати комп’ютерну емуляцію мереж передачі даних;

досвід:

– експлуатації засобів передачі даних та інших систем документального електрозв’язку;

– аналізу перспективних напрямків розвитку засобів і мереж передачі даних та інших систем документального електрозв’язку.

ТЕМА 1
СПОСОБИ ПЕРЕТВОРЕННЯ І ПЕРЕДАЧІ ЦИФРОВИХ СИГНАЛІВ ДАНИХ

ЛЕКЦІЯ 1
ІНФОРМАЦІЯ В СИСТЕМІ ПЕРЕДАЧІ ДАНИХ

1.1. Загальна характеристика дисципліни

Предметом навчальної дисципліни є вивчення особливостей побудови та оволодіння навичками експлуатації засобів систем передачі даних спеціального зв'язку і загального застосування.

Зміст дисципліни (таблиця 1.1):

Таблиця 1.1

Форма навчання	Семестр	Всього кредитів/годин	Розподіл навчального часу за видами занять				Семестрові атестація
			Лекції	Практичні (семінарські) заняття	Лабораторні роб. (комп.пр., практ. на техн.)	СРК	
Денна	Всього	5/150	12	32	10	96	
	8	4/120	12	32	10	66	залік
	КР	1/30				30	захист КР

Розділ (блок змістовних модулів) 1. **Принципи побудови систем і апаратури передачі даних та організації роботи мереж. Завадостійке кодування**

Тема 1. Способи перетворення і передачі цифрових сигналів даних.

Домашня розрахункова робота.

Тема 2. Завадостійке кодування в системах передачі даних.

Тема 3. Принципи побудови апаратури та мереж передачі даних.

Модульна контрольна робота.

Залік.

Рейтинг курсанта з кредитного модуля складається з балів, що він отримує за:

1) роботу на практичних заняттях: **2** відповідей (в кожного курсанта мінімум) на **9** практичних заняттях (за умови, що на одному занятті опитуються 4…6 курсантів при максимальній чисельності групи 25…30 осіб – (9пз × 4…6 курсантів):(25…30 курсантів) ≈ **2** відповідей);

2) виконання 4 практичних завдань на комп'ютерних практикумах (3/2, 3/4, 3/6, 3/10)

3) **1** модульну контрольну роботу (МКР), яка складається з **3** письмових експрес-контролів в кінці 1, 2, 3, тем кредитного модуля, які виконуються протягом 30 хвилин);

Робота курсанта в семестрі оцінюється наступним чином:

1. Робота на практичних заняттях (кількість відповідей в кожного курсанта мінімум – 2)

Ваговий бал – **5**.

Максимальна кількість балів – **10**.

Критерії оцінювання:

5 *– все вірно, відповідь без зауважень, традиційна оцінка– відмінно;*

4 *– вірно, але не повністю, відповідь з незначними помилками – традиційна оцінка добре;*

2…3 *– відповідь має певні недоліки, потребує корективи та поправки з боку викладача або курсантів, традиційна оцінка – задовільно;*

1 *– відповідь має явні недоліки, потребує значні корективи та поправки з боку викладача, хоча пояснення в вірному напрямку;*

0 *– немає відповіді або відповідь не вірна, традиційна оцінка– незадовільно.*

2. Виконання 4 практичних завдань на заняттях з технікою (3/2, 3/4, 3/6, 3/10) (кількість оцінок у кожного курсанта – 4)

Ваговий бал – **5**.

Максимальна кількість балів – **20**.

Критерії оцінювання:

5 *– все вірно, відповідь без зауважень, традиційна оцінка– відмінно;*

4 *– вірно, але не повністю, відповідь з незначними помилками – традиційна оцінка добре;*

2…3 *– відповідь має певні недоліки, потребує корективи та поправки з боку викладача або курсантів, традиційна оцінка – задовільно;*

1 *– відповідь має явні недоліки, потребує значні корективи та поправки з боку викладача, хоча пояснення в вірному напрямку;*

0 *– немає відповіді або відповідь не вірна, традиційна оцінка– незадовільно.*

3. Модульний контроль (кількість – 1)

Ваговий бал – **15**.

Максимальна кількість балів – **15**.

МКР складається з **3** письмових експрес-контролів, які виконуються на протязі від 30 хвилин на завершальному занятті кожної теми. Кількість балів за МКР складає суму кількості балів ПЕК (**15 = 3×5**), що входять до його складу.

Критерії оцінювання ПЕК:

5 – відповіді на обидва питання вірні, без зауважень, традиційна оцінка– відмінно;

4 – одне питання вірно, але друге не повне, відповідь з помилками – традиційна оцінка добре;

2…3 –відповіді на обидва питання мають певні недоліки, потребують корективів, традиційна оцінка – задовільно;

1 – відповіді на одне з питань не має, а на інше має явні недоліки, потребує значні корективи , традиційна оцінка – задовільно;

0 – немає відповідей на обидва питання або відповіді не вірні, традиційна оцінка– незадовільно.

Розрахунок шкали (R) рейтингу:

Максимальний рейтинг за семестр складає **100 балів.**

Так як сума вагових балів контрольних заходів протягом семестру складає:

R_D= 10 (2 відповіді ×5) +20 (4 завдання ×5) + 15 (1 МКР ×15) = 10+20+15=45

Для отримання стандартизованого балу вводиться підвищуючий коефіцієнт 0,45 (R_C= **45** / 0,45 = **100 балів**).

Штрафні та заохочувальні бали: Сума як штрафних, так і заохочувальних балів не має перевищувати $0{,}1\times R_D=0{,}1\times 100\approx 10$.

Заохочувальні бали:

За вдосконалення методичної бази навчальної дисципліни та матеріальної бази кафедри можна заробити до **10** балів.

За виступ на конференції, конкурсну роботу, поданим заявкам на патент можна отримати до **10** балів.

Штрафні бали:

За недоліки при виконанні навчального плану можна отримати штрафні (негативні бали) відповідно ваговим балам по видам занять.

Необхідною умовою допуску до заліку є:

1. Виконання 4 практичних завдань на заняттях з технікою

Курсанти, які набрали впродовж семестру необхідну кількість балів ($R_D \geq \mathbf{0{,}6}R_D$) (**≥60 балів**), мають можливість отримати загальну оцінку автоматично, відповідно до набраного рейтингу (таблиця 1.2).

Якщо їх не влаштовує набрана кількість балів, вони мають можливість її підвищити, шляхом виконання залікової контрольної роботи.

Залік письмовий виконується за жорсткою системою (тобто результати навчання в семестрі не враховуються).

Таблиця 1.2

Бали рейтингу						**Критерії**	**Оцінка**
семестровий *RD*			***RD*· 0,45**				
43	…	45	95	…	100	$0{,}95\cdot R \le RD$	відмінно
39	…	42	85	…	94	$0{,}85\cdot R \le RD < 0{,}95\cdot R$	дуже добре
34	…	38	75	…	84	$0{,}75\cdot R \le RD < 0{,}85\cdot R$	добре
30	…	33	65	…	74	$0{,}65\cdot R \le RD < 0{,}75\cdot R$	задовільно
27	…	29	60	…	64	$0{,}6\cdot R \le RD < 0{,}65\cdot R$	достатньо

Максимальна кількість балів, яку може отримати курсант за залікову контрольну роботу **100 балів (в білеті 3 питання – перше і друге питання по 30 балів, третє питання 40 балів)**.

Підсумкова оцінка за залік (традиційна) виставляється згідно таблиці 1.3.

Таблиця 1.3

Сумарний рейтинг RD	**Оцінка**
95…100	відмінно
85…94	дуже добре
75…84	добре
65…74	задовільно
60…64	достатньо
Сумарний рейтинг ≤ 59	незадовільно
Не виконані умови допуску	не допущено

1.2. Поняття документального електрозв’язку. Область використання

Інформація відіграє значну роль у житті сучасного суспільства та держави. Від своєчасності доставки та якості інформаційного забезпечення у значній мірі залежить як розвиток більшості галузей економіки так і безпека держави в цілому.

Особлива роль в цьому напрямку належить засобам, що забезпечують реалізацію документального зв’язку, тобто зв’язку, при якому відправник інформації має документальне підтвердження про факт, зміст, час передачі та у багатьох випадках квитанцію про надходження даної інформації до отримувача.

Документальний електрозв’язок (згідно ДСТУ 2619–94) – це вид електрозв’язку за допомогою якого здійснюється передача документальних повідомлень у вигляді літерно-цифрових текстів, цифрових даних і графічних зображень з подальшим відтворенням їх на прийомі на певних матеріальних носіях інформації.

Види документального електрозв’язку:

1. ТЛГ зв’язок – служба доставки повідомлень в буквено-цифровому вигляді, а також комплекс послуг, що надаються населенню та підприємствам при використанні системи телеграфного зв’язку

Телеграфна мережа загального користування надає населенню і підприємствам комплекс послуг з прийому, передачі і доставці адресатам повідомлень, що надходять у відділення зв’язку. При надходженні заявки на передачу телеграми оператор відділення зв’язку по каналах телеграфного зв’язку передає повідомлення іншому відділенню зв’язку, найбільш близько розташованому до адресата . Після прийому телеграфного повідомлення іншим відділенням зв’язку телеграма передається адресату службою доставки пошти.

2. Передача даних – вид ДЕЗ, який забезпечує обмін дискретною інформацією, поданою у формалізованому вигляді та призначеною для опрацювання обчислювальними машинами чи вже опрацьованої ними

Отже передача даних відбувається в межах так званих комп’ютерних мереж.

Комп’ютерна мережа (обчислювальна мережа, мережа передачі даних) – система зв’язує комп’ютери і/або комп’ютерне устаткування (сервери, маршрутизатори і інше устаткування) через фізичне з’єднання або канали зв’язку.

Комп’ютерна мережа структурно має дві складові: комунікаційну та інформаційну.

Комунікаційна складова забезпечує власне передачу даних, виконує завдання, пов’язані з їх перетворенням.

Інформаційна складова призначена для зберігання і обробки інформації. На базі одної комунікаційної складової може бути побудована група інформаційних.

3. Телематичні служби ДЕЗ (ТМ) – служби ДЕЗ, за винятком телеграфного зв’язку та служби передачі даних, призначені для передачі інформації через мережі електрозв’язку. Прикладами ТМ служб ДЕЗ є: факсимільні служби, служби електронних повідомлень, а також служби доступу до інформації, що зберігається в електронному вигляді.

Телематичні (від «телекомунікації» і «інформатика») служби призначені для обміну інформацією між різними об’єктами, машинами і людьми.

Факсимільний зв’язок – це ТМ служба передачі та відтворення будь-якого нерухомого графічного зображення.

Електронна пошта – ТМ служба, призначена для обміну електронними повідомленнями з проміжним накопиченням між абонентськими терміналами.

Служба доступу до інформаційних ресурсів – вид ТМ служби, призначеної для отримання інформаційного ресурсу користувачем по його ініціативи, вираженої у формі запиту, а також надання послуг розміщення і

зберігання інформаційного ресурсу, отриманого від постачальника (наприклад, служби WWW).

Наприклад: Служби документального електрозв'язку ВАТ "Укртелеком" забезпечують надання таких послуг, як:

- передача телеграм;
- абонентське телеграфування;
- телекс;
- факсимільний зв'язок;
- передача газетних шпальт;
- електронна пошта Internet.

1.3. Інформація, форма її подання

Інформація – це одиничні повідомлення або їх сукупність, які знімають невизначеність, яка існує до їх приходу. Якщо повідомлення не знімають невизначеність, вони можуть бути віднесені до інформаційних шумів. Якщо повідомлення збільшує невизначеність, то вони несуть в собі дезінформацію.

Іншими словами, **інформація** – це нові знання, які отримує споживач (суб'єкт) у результаті сприйняття і обробки певних відомостей.

Інформацію прийнято класифікувати:

І. За способом сприйняття:

Для людини інформація поділяється на види залежно від типу рецепторів, що сприймають її.

- Візуальна – сприймається органами зору. Ми бачимо все довкола.
- Акустична – сприймається органами слуху. Ми чуємо звуки довкола нас.
- Тактильна – сприймається тактильними рецепторами.
- Нюхова – сприймається нюховими рецепторами. Ми відчуваємо аромати довкола.
- Смакова – сприймається смаковими рецепторами. Ми відчуваємо смак.

ІІ. За формою подання:

За формою подання інформація поділяється на такі види:

- Текстова – що передається у вигляді символів, призначених позначати лексеми мови.
- Числова – у вигляді цифр і знаків, що позначають математичні дії.
- Графічна – у вигляді зображень, подій, предметів, графіків.
- Звукова – усна або у вигляді запису аудіоповідомлення.

ІІІ. За призначенням:

- Масова – містить тривіальні відомості і оперує набором понять, зрозумілим більшій частині соціуму.
- Спеціальна – містить специфічний набір понять, при використанні відбувається передача відомостей, які можуть бути не зрозумілі основній

масі соціуму, але необхідні і зрозумілі в рамках вузької соціальної групи, де використовується дана інформація.

– Особиста – набір відомостей про яку-небудь особистість, що визначає соціальний стан і типи соціальних взаємодій всередині популяції.

У телекомунікаційних мережах інформація передається у вигляді повідомлень, які в залежності від виду зв'язку можуть мати форму:

– телеграми (шифрограми) при телеграфному зв'язку;
– кодограми при передачі даних;
– зображення при факсимільному зв'язку;
– лист електронної пошти при e-mail.

В системах передачі повідомлення передаються у формі сигналів з визначеними фізичними властивостями. В загальному випадку **сигнал** – це будь-яка зміна початкового стану об'єкту, яка може викликати реакцію людини чи приладу (електросигнал, радіосигнал і т.д.). В свою чергу в сигналі інформація передається шляхом зміни (модуляції, маніпуляції) одного з його параметрів (амплітуди, частоти, фази або комбіновано) за законом зміни інформаційного сигналу.

1.4. Кількість інформації, одиниці її виміру

Вимірювання інформації може розглядатися як визначення її кількості і обсягу даних. Залежно від форми адекватності інформації ці параметри мають різну інтерпретацію.

Синтаксична міра інформації не висловлює смислового ставлення до об'єкта, і обсяг даних в повідомленні вимірюється кількістю символів (розрядів) в електронному листі. У двійковій системі кількість розрядів вимірюється в бітах, в десятковій системі числення – в дітах. Так, повідомлення в десятковій системі числення у вигляді числа 57 332 має об'єм даних 5 дит, а повідомлення в двійковій системі 01101111 – 8 біт. Кількість інформації на синтаксичному рівні пов'язано з поняттям невизначеності стану системи (ентропії системи), яке було сформульовано К. Шенноном, і вимірюється зміною (зменшенням) невизначеності системи.

Для вимірювання смислового змісту інформації на семантичному рівні застосовується Тезаурусний міра.

Тезаурус – сукупність відомостей, якими володіє користувач або система.

Прагматична міра інформації визначає корисність інформації для досягнення користувачем поставленої мети.

Біт – мінімальна одиниця виміру інформації, кількість інформації, яким описується стан "включений" (1) або "вимкнений" (0). Слово "біт" походить від Binary Digit (двійкова цифра). Саме таке визначення одиниці "біт" і дано вище в підрозділі "Кодування чисел". Чи є електрична напруга на висновках схеми, чи є електричний заряд в комірці пам'яті, яке з двох можливих протилежних напрямків намагніченості в даній області магнітного носія, чи відображає світло лазерний оптичний диск - все це питання, які

потребують відповіді Так або Ні, один з яких трактується як логічна одиниця, а другий - як логічний нуль, тому електронний спосіб рахунку заснований всього на двох цифрах, 0 і 1. Саме дані в форматі цих цифр доручається зберігати комп'ютерної пам'яті і обробляти обчислювальної системі.

Байт – одиниця вимірювання кількості інформації, обсягу пам'яті і ємності накопичувача. У пам'яті ЕОМ байт – найменша адресується одиниця даних, що обробляється як єдине ціле (в перших комп'ютерах за раз могло оброблятися число довжиною 8 біт), тому в якості одиниці виміру обсягу комп'ютерної інформації обрана більша, ніж біт, одиниця інформації - байт, послідовність 8 біт, тобто 1 байт = 8 біт.

В символьних (текстових) даних кожен символ кодується (позначається) одним байтом. Унікальне 8-бітове позначення (код) отримують великі і малі літери англійського і російського алфавітів, цифри від 0 до 9, знаки пунктуації, інші символи (відсоток, номер) і деякі керуючі коди передачі інформації. На одній машинописної сторінці при розміщенні 50 рядків і 60 символів тексту в одному рядку міститься 3 тис. Символів, отже, для зберігання такого тексту буде потрібно 3 тис. Байт машинної пам'яті.

Для запису чисел коротше 8 біт в байтах додаються зліва нулі. Ліві нулі не змінюють двійковечисло, але створюють єдину форму запису чисел – 8 біт на будь-яке число від 0 до 255.

У десятковій системі числення укрупнені одиниці виміру позначаються приставками до назви кіло, Мега, Гіга, що відповідає збільшенню чисельного значення на множник десять в ступені: 103 = 1000 (тисяча), 106 = 1 000 000 (мільйон), 109 = 1 000 000 000 (мільярд), тобто перехід до наступної, більшої, одиниці супроводжується множенням па 1000 (103). У двійковій системі укрупнені одиниці виміру теж позначаються приставками до назви кіло, Мега, Гіга, Тера, Пета, ЕКЗА, але вони збільшують чисельне значення на множник 2 в ступені: 210, 220, 230, 240, 250, 260, тобто перехід до наступної, більшої, одиниці супроводжується множенням на 210 = 1024:

- 1 Кбайт = 1024 байт = 210 байт;
- 1 Мбайт = 1024 Кбайт = 220 байт;
- 1 Гбайт = 1024 Мбайт = 230 байт;
- 1 Тбайт = 1024 Гбайт = 240 байт;
- 1 Пбайт = 1024 Гбайт = 250 байт;
- 1 Ебайт = 1024 Пбайт = 260 байт.

Передача інформації з каналів зв'язку характеризується швидкістю передачі даних: біт в секунду, Кбіт / с, Мбіт / с і ін. Кількість переданих біт зручніше вважати в десятковій системі числення, тому приставки в одиницях виміру швидкості пов'язані коефіцієнтом 1000 (103). Одиниця виміру швидкості передачі даних 1 біт / с називається *Бодом.*

1.5. Структура та параметри систем передачі даних

Сукупність кінцевої АПД і каналу (каналів), які забезпечують обмін даних між двома елементами мережі, називають системою передачі даних (СПД).

СПД – є вторинною системою електрозв'язку і використовує для передачі канали, що утворюються первинними (транспортними) системами передачі.

Модель СПД даних можна представити у такому вигляді (рисунку 1.1):

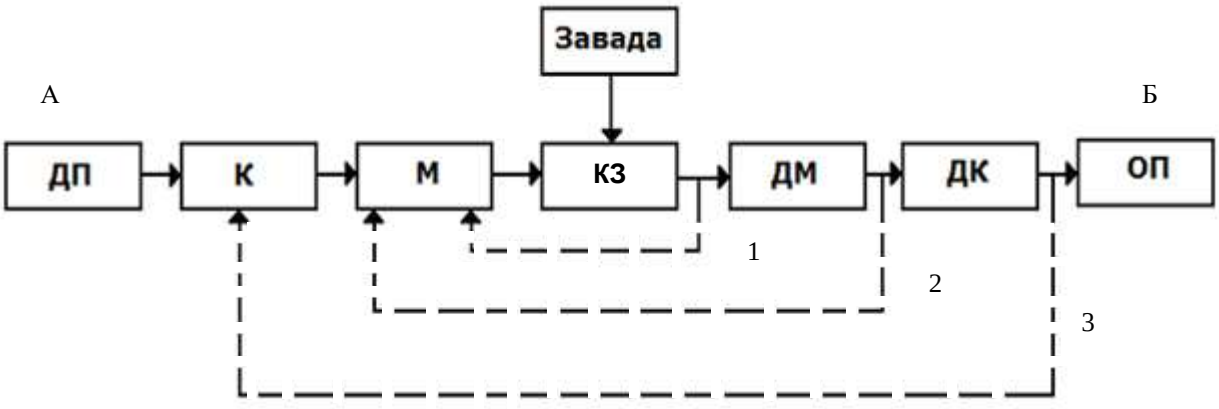


Рисунок 1.1 – Модель системи передачі даних

де ДП – джерело повідомлення; К – кодер; М – модулятор; КЗ – канал електрозв'язку; ДМ – демодулятор; ДК – декодер; ОП – одержувач повідомлення.

Кодер забезпечує захист інформації від помилок (завадостійке кодування).

Модулятор – перетворення сигналів до вигляду придатного для передачі у певному каналі зв'язку.

За використовуємою моделлю системи передачі даних можна розділити на дві групи: системи без зворотного зв'язку і системи зі зворотним зв'язком.

До першої групи відносяться СПД, що використовують для передачі інформації прості (ненадлишкові) коди, і СПД, що використовують надлишкові коди, що виявляють і виправляють помилки. СПД з застосуванням простих кодів не можуть забезпечити високої достовірності переданої інформації через низьку завадостійкість прийому повідомлень в умовах дії завад. Такі системи знаходять застосування головним чином при передачі інформації на короткі відстані при низькому рівні завад у каналі зв'язку.

Ускладнення кодів (збільшення надмірності) покращує ефективність проте вимагає значних ресурсів пропускної здатності. У той же час навіть прості коди завжди мають кращі властивості щодо виявлення помилок аніж їх виправлення.

Тому до другої групи СПД (зі зворотним зв'язком) відносяться системи, у яких якість передачі інформації контролюється і керується за допомогою використання каналу зворотного зв'язку. Як правило, у таких системах застосовують коди, що виявляють помилки. Перевагою СПД зі зворотним зв'язком є можливість підвищення правильності переданої інформації без ускладнення коду, використовуваного в системі, простою зміною функцій зворотного каналу. У таких системах по прямому каналу передають повідомлення від станції А до станції Б. Зворотний же канал у СПД може бути використаний для посилки передавальному пристрою А відомостей про фактичний прийом повідомлень на станції Б. В залежності від охоплення певного обладнання СПД її зворотний зв'язок розрізняють за трьома типами (рис. 1): тип 1 – фіксує факт надходження сигналу (наявності необхідного рівня) з лінії зв'язку на вхід приймача чи після проходження сигналом перших каскадів приймача; тип 2 – фіксує правильність розпізнавання одиничних елементів сигналу демодулятором (охоплює модем); тип 3 – фіксує правильність прийому кодових комбінації (охоплює всю систему).

Варіант 1 зворотного зв'язку фактично контролює якість прямого каналу, і в залежності від його стану передавач може змінювати умови передачі сигналів (метод кодування, вид модуляції, швидкість передачі, потужність сигналу і т.д.). Варіант 2 – зворотні зв'язки контролюють роботу модему, правильність демодуляції сигналів. Варіант 3 – зворотні зв'язки контролюють роботу декодера. Таким чином, у варіантах 2 і 3 зворотний зв'язок контролює рішення, прийняті приймачем.

У залежності від використання зворотного зв'язку СПД кожного з трьох типів поділяють на системи з інформаційним зворотним зв'язком (ІЗЗ) і з вирішальним зворотним зв'язком (ВЗЗ).

ВЗЗ (вирішальний зворотний зв'язок) – рішення про правильність прийнятої інформації виноситься приймачем і у зворотному каналі видається підтвердження правильності прийому або запит на повторення неприйнятої інформації. При цьому використовуються прості коди , а у зворотному каналі кількість передаваємої інформації незначна.

ІЗЗ (інформаційний зворотний зв'язок) – рішення про правильність прийнятої інформації видає передавач на основі переданої і прийнятої зі зворотного зв'язку інформації. Процес повторюється доти поки інформація не збігається. З ІЗЗ можна передавати без кодів, але у зворотному каналі здійснюється повна передача всього обсягу інформації.

Загальна структура СПД приведена на рисунку 1.2.

Кодек виконує функції кодування сигналів завадостійким кодом та реалізує алгоритми підвищення достовірності передачі.

Модем виконує функцію узгодження сигналу передачі даних з параметрами каналу передачі, в ньому відбувається модуляція (демодуляція) сигналу, а також забезпечення параметрів стандартного стику з каналом передачі (кількість ланцюгів, електричні параметри сигналу і ін.)

Для оцінки і порівняльного аналізу СПД використовують параметри:

– формат повідомлення;
– достовірність;
– швидкість передачі інформації;
– час затримки повідомлення.

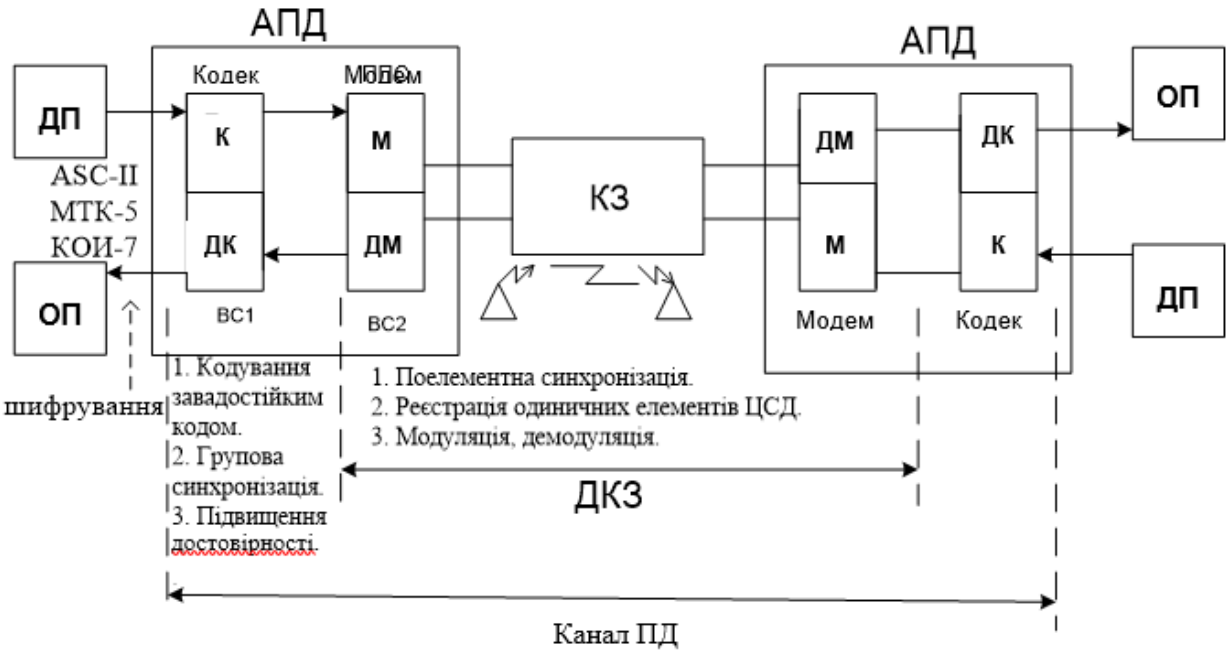


Рисунок 1.2 – Загальна структура СПД

1) Формат повідомлення визначає порядок розташування символів даних у повідомленні таким чином, щоб можливо було забезпечити автоматичну обробку при підготовці до передачі, прийомі та в процесі переміщення в мережі.

2) Достовірність характеризується:

– ймовірністю помилкового прийому кодової комбінації первинного коду $P_{пом}$ (l) (або Р);

– ймовірністю стирання кодової комбінації $P_{стир}$ (l) (при виявленні помилки);

– ймовірністю вірного прийому кодової комбінації $P_{вір}$:

$$P_{пом} + P_{стир} + P_{вірного} = 1$$

Міжнародні норми на $P_{пом} \approx 10^{-3} - 10^{-5}$ для ТГ зв'язку, $\approx 10^{-6} \div 10^{-9}$ для ПД.

3) Швидкість передачі інформації – R [біт/с] – це середня кількість інформації (біт), що передається за одиницю часу (сек.):

$$R = \frac{H}{t_0},$$

де H – ентропія джерела інформації; t_0 – довжина одиничного елементу.

При рівноймовірному алфавіті формула ентропії приймає вигляд:

$$H = -\log\frac{1}{m} = \log m,$$

де $p(a) = \frac{1}{m}$ – ймовірність появи певного символу на виході джерела інформації (m – кількість символів в алфавіті).

При використанні одиниць вимірювання кількості інформації в бітах та двійкового коду передачі (m=2), маємо H=1, тоді

$$R = \frac{1}{t_0} = B\left[\frac{1}{c}\right].$$

Для нерівноймовірних і взаємозалежних сигналів повідомлення

$$R = \frac{\sum p \cdot \log_2 p}{t_0}.$$

Максимальна швидкість передачі інформації по ДКЗ визначає **пропускну здатність (ПЗ):**

$$C = \frac{1}{t_0}\left[\log_2 m + \log_2\frac{1}{mp} + (1-P)\log_2(1-P)\right] \text{ біт/с},$$

Технічна ПЗ

Додадок до інф. ПЗ за багатознач.

Додадок до інф. ПЗ за якість обсл.

де P – ймовірність відмови у передаванні за рахунок комутаційного обладнання.

При m=2 ця формула приймає вигляд.

$$C = \frac{1}{t_0}\left[1 + \log_2\frac{1}{2p} + (1-P)\log_2(1-P)\right].$$

4) **Час затримки повідомлення** ($t_{затр}$) – час від моменту надходження повідомлення на вхід СПД до моменту його видачі отримувачу. Як правило це випадкова величина і її задають виходячи із вимог системи управління в інтересах якої створена СПД як імовірнісну функцію $p\left[t_{затр} \le \tau_{зад}\right]$

Основним напрямком підвищення вірогідності ПД є застосування завадостійких кодів. На сьогодні відомі десятки кодів, які можуть виявляти і виправляти помилки (одиночні, двійні і т.д.).

ЛЕКЦІЯ 2
СПОСОБИ ПЕРЕДАЧІ ДИСКРЕТНИХ СИГНАЛІВ ПО КАНАЛАМ ЗВ'ЯЗКУ

2.1. Синхронні та асинхронні способи передачі

При здійсненні схемної реалізації СПД виникає завдання забезпечення синхронної роботи передавальної та приймальної частини (рисунок 1.3), з метою точного визначення оптимального моменту реєстрації прийнятого імпульсу та місце цього імпульсу в кодовій комбінації.

Рисунок 1.3 – Синхронна робота передавальної та приймальної частини СПД

В у відповідності до способу підтримання синхронізації в СПД розрізняють два способи передачі інформації:

– синхронний – коли кодові комбінації прямують одна за одною, мають однакову кількість однакових елементів;

– асинхронний – коли значуща позиція кожного елемента залежить від значущої позиції раніше прийнятого елемента.

Асинхронні системи в свою чергу бувають:

– старт-стопні;

– асинхронні попакетні.

В старт-стопних системах фаза між розподілювачами передавача і приймача підтримується в межах одного циклу роботи. Розподілювачі запускаються на 1 цикл і по його закінченню зупиняються. Передано 1 знак і розподілювачі стають на стоп.

Розходження фаз, яке виникає внаслідок нестабільності пристроїв, ліквідується під час зупинки розподілювачів. Потім розподілювачі запускаються по новому на новий цикл передачі і т.д. Так як за 1 цикл розподілювачі передавача і приймача не можуть розійтися по фазі на значну величину, то їх старт-стопні схеми корегування фази будуються достатньо простими.

Старт-стопний спосіб використовують в телеграфному зв'язку. Отже при відсутності для передачі знаку розподілювач передавача (і приймача)

«стоїть на стопі», тобто через апарат (лінійне його коло проходить струм (50 мА)).

Після натискування на клавішу необхідно для передачі знаку (літери, цифри) стартує передаючий розподілювач і в канал (лінію) зв'язку передається стартова посилка (безструмова).

Після стартової посилки (рисунок 1.4) передаються п'ять посилок (розрядів) КК первинного коду даного знаку («і» – наприклад). По закінченню передачі апарат стає на стоп, а в лінію передається «стопова» (струмова) посилка довжиною $1{,}5 \cdot \tau_0$. Збільшення довжини стопової посилки обумовлене вимогою надійно поставити апарат «на стоп» щоб він не стартував по новому, інакше буде знову передано той самий знак «і».

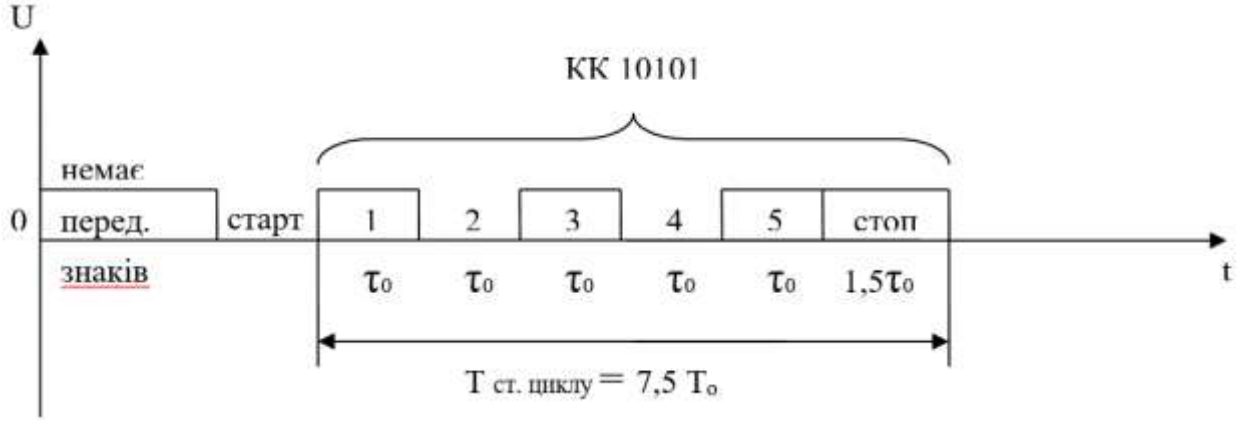


Рисунок 1.4. – Передача п'ятьох посилок (розрядів) КК первинного коду

Стартова посилка потрібна щоб запускати прийомний розподілювач і потім зареєструвати 5 інформаційних символів (посилок).

Стопова (струмова) посилка потрібна для надійної зупинки прийомного розподілювача. Фазування по циклам здійснюється стартовою і стоповою посилками.

Стартовий і стоповий імпульси є корегуючими.

При передачі знаку апарат стає на «стоп» і передається струмова посилка. За час прийому стопової посилки ліквідується розходження фаз між передаючим і прийомним розпределювачами. Простий і надійний спосіб передачі. Але низькошвидкісний.

При асинхронному по пакетному способі передачі (рисунок 1.5) данні передаються у вигляді пакету (подібно до кодової комбінації старт-стопного методу, але більшої довжини). Пакет даних традиційно має заголовок та ознаку закінчення, але крім того на початку заголовку додаються корегуючі сигнали – поелементної (тактової) синхронізації та фазування (циклової) синхронізації. Класичний приклад таких систем **радіоEthernet**.

В синхронних системах фаза розподілювачів передавача і приймача підтримується постійно, так як цикли їх роботи здійснюються безперервно незалежно є інформація для передачі, чи її не має.

Рисунок 1.5 – Асинхронний попакетний спосіб передачі даних

В синхронних системах більш високі вимоги до підтримки фази прийомного розподілювача відносно передаючого, тому в більшості синхронних систем застосовується примусова підстройка фази (по корегуючим імпульсам, що постійно передаються по каналу). Схеми корегування фази значно складніші.

При синхронному попакетному способі передачі одиничні елементи цифрової системи даних (ЦСД) кодових комбінацій (знаків) передаються один за одним безперервно (рисунок 1.6).

Це дає можливість у приймачі попередньо передбачити час прийому кожного одиничного елементу ЦСД, що несе інформацію про ту чи іншу літеру і забезпечити правильну його реєстрацію.

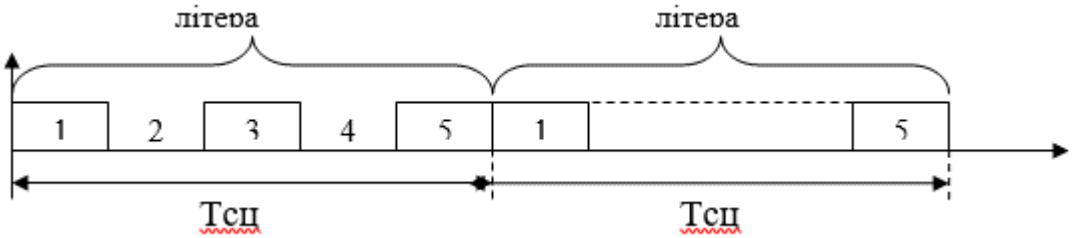


Рисунок 1.6 – Синхронний попакетний спосіб передачі даних

В синхронних системах між двома значимими моментами зберігається ціле число одиничних інтервалів (рисунок 1.7).

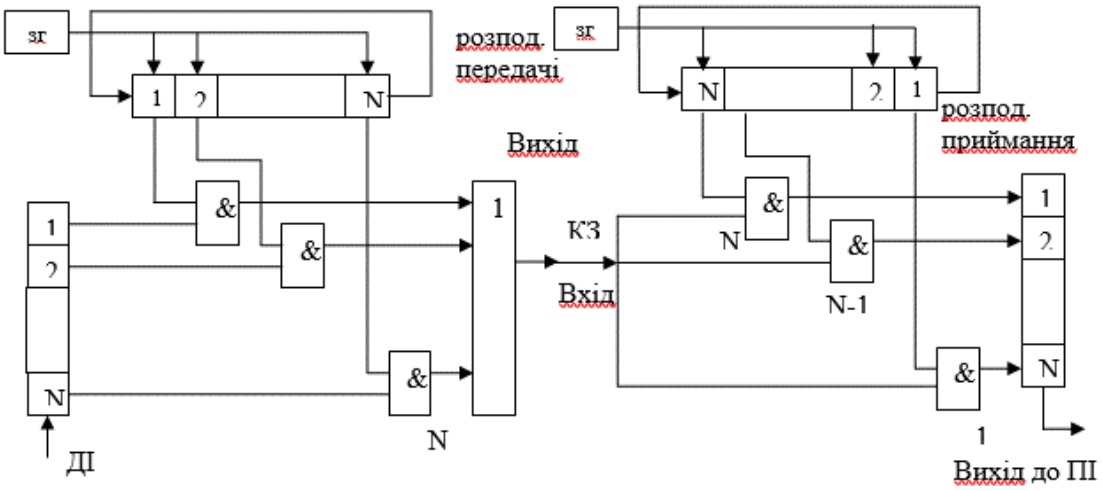


Рисунок 1.7 – Структурна схема синхронної системи передачі

В синхронних системах більш високі вимоги до системи синхронізації. На прийомі потрібно знати коли приходить 1,2,……n розряд КК, що

приймається (рисунок 1.8). Це в свою чергу вимагає високої стабілізації частоти ЗГ.

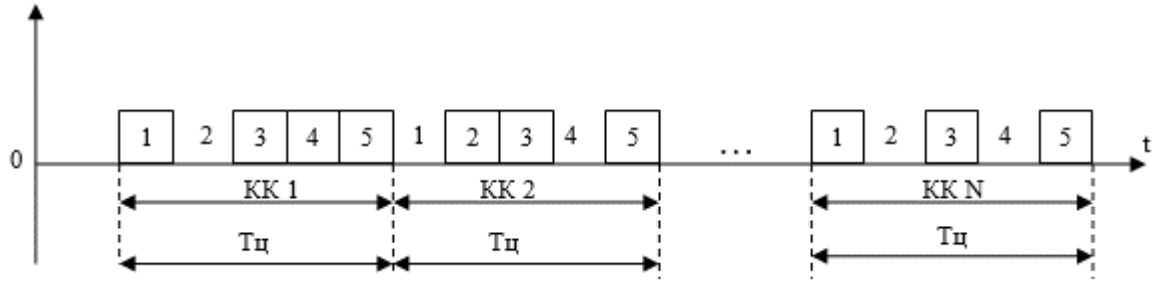


Рисунок 1.8 – Часова діаграма сигналу синхронізації системи передачі

Система синхронізації забезпечує умову, що в час прийому 1 розряду КК відкрита схема $\&_1$ приймача (тобто сигнал 1 в n-розряді розподілювача поступає на перший вхід, на другий вхід якої поступає 1 розряд КК зі входу приймача).

При прийомі 2-го розряду КК відкрита схема $\&_2$ і т.д.

Якщо з кільця розподілювача приймача не будуть погоджено подаватися сигнали управління на схеми, то правильний прийом розрядів КК стане неможливим.

Таким чином **необхідна поелементна і групова синхронізація**.

Переваги синхронних систем (способу передачі):

– Постійна готовність до передачі КК (знаків).

– Є можливість забезпечити гарантовану стійкість кодування (захист).

– Забезпечується більш висока завадостійкість.

– Більш ефективно використовується пропускна спроможність КЗ.

– Є можливість побудувати багатократні системи передачі.

Недоліки синхронного способу передачі:

– Більша складність реалізації синхронних пристроїв передачі за рахунок, в першу чергу, складних пристроїв синхронізації (по елементної і групової).

– Обмежується швидкість роботи джерела інформації (видача знаків від ДІ на вхід передавача в такт з прийнятою швидкістю передачі).

На сьогодні синхронні способи передачі використовуються в АПД та СА при високошвидкісній передачі даних (ПД).

2.1. Методи реєстрації дискретних сигналів

Реєстрація – встановлення значущої позиції («0» чи «1») кожного прийнятого одиночного елемента ЦСД (на виході детектора приймача)

Вирішуючий пристрій або реєструючий пристрій це пристрій який здійснює цю процедуру реєстрації.

В залежності від алгоритму роботи реєструючого пристрою (РП) вони можуть бути:

– РП без стирання, → «1» або «0» на виході.
– РП зі стиранням → «1» або «0» сигнал не визначено (стирається).

Сигнали в КЗ за рахунок не ідеальності їх характеристик, наявності рідного роду завад пошкоджуються і в пошкодженому вигляді поступають в приймач це суттєво впливає на якість реєстрації.

Після перетворень і демодуляції вхідний дискретний сигнал відрізняється від переданого. Ці пошкодження полягають в тому, що значущі моменти (ЗМ) прийнятого сигналу за рахунок дії завад не співпадають з переданими та мають викрівлення. Можуть зміститися значущі моменти, а можуть появитися і додаткові пари значущих моментів.

Відомі два види пошкоджень:
– крайові пошкодження;
– дроблення.

Крайові пошкодження – це пошкодження обумовленні зміщенням значущих моментів відносно їх ідеального розміщення.

Крайові пошкодження можуть бути (рисунок 1.9):
– двосторонні;
– односторонні.

$$\delta_{кр} = \frac{Q_i}{T_o}$$

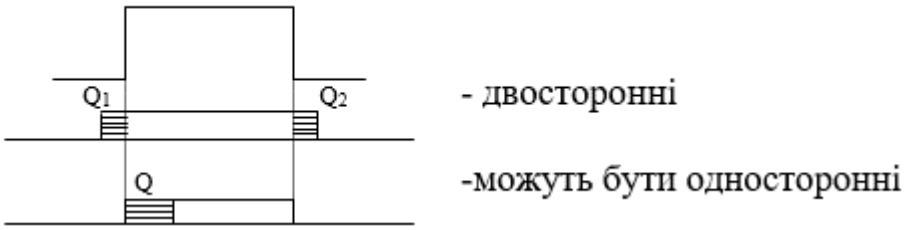


Рисунок 1.9 – Види крайових пошкоджень

Також крайові пошкодження можуть бути:
– регулярні;
– випадкові.

Дроблення – це пошкодження, що обумовленні появою додаткових пар значущих моментів.

Дроблення поділяються (розрізняються):
– довжиною дроблень;
– моментами часу початку дроблень.

Дроблення на відміну від крайових пошкоджень завжди випадкові (рисунок 1.10).

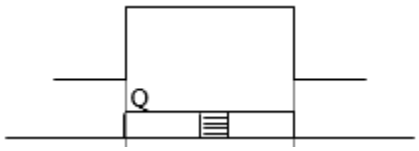


Рисунок 1.10 – Вид випадкового дроблення

Основними параметрами реєструючого пристрою (РП) **є виправляюча спроможність.**

Виправляюча спроможність – це можливість пристрою правильно реєструвати одиничний елемент при наявності пошкоджень в ньому. Чисельно виправляюча спроможність рівна тій найбільшій величині пошкоджень приймаємого імпульсу, при якій іще можлива його правильна реєстрація.

Розрізняють виправляючу спроможність:

– при крайових пошкодженнях – $\mu_{кр}$

– при дробленнях – $\mu_{др}$

При дробленнях виправляюча спроможність $\mu_{др}$ визначається не тільки величиною $\delta_{др}$ (τ), але і моментах часу їх появи.

Відомі **два методи реєстрації** одиночних елементів ЦСД:

– метод стробування;

– інтегральний метод.

Реєстрація методом стробування

Сутність методу в тому, що одиночний елемент аналізується не на всьому інтервалі одиночного елементу T_o, а деякій його частині $t_a < T_o$ (рисунок 1.11).

При цьому значима позиція одиночного елементу до початку аналізу і після винесення рішення не враховується. Взагалі час аналізу сигналу $t_a << T_o$ і розміщується на середині одиночного елемента ЦСД, як найменш пошкодженої частини.

Поріг реєстрації сигналу вибирають рівень половині номінального значення амплітуди сигналу $\frac{1}{2}U_o$.

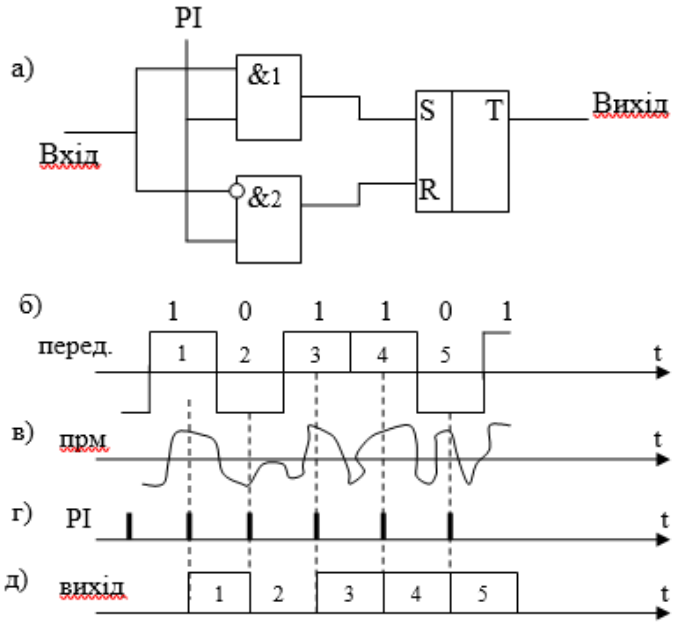


Рисунок 1.11 – Схеми реалізації

Виправляюча спроможність РП, реалізуючого методу стробування при крайових пошкодженнях може бути визначена за допомогою:

$$\mu_{кр} = \frac{T_o - t_a}{2T_o} \times 100\% \quad (\text{при } t_a \to 0, \text{ то } \mu_{кр}=50\ \%)$$

Якщо дроблення співпадає з моментом реєстрації тоді $\mu_{др} \approx 0$

Реєстрація методом стробування використовується:

– в низькошвидкісних ППС;
– в старт-стопних апаратах.

Реєстрація інтегральним (аналоговим) методом

Суть інтегрального методу в тому, що одиничний елемент аналізується на інтервалі $t_a < T_o$ і рішення приймається по критерію більшості. На конденсаторі накопичується енергія (пост. часу RC вибирається = (3-5) T_o, це забезпечує лінійне зростання заряду за час аналізу (рисунок 1.12)

Управління роботою RC і визначення результату за $t_{ан}$ здійснюється за рахунок порогового пристрою.

Якщо на більшій частині інтервалу аналізу t_a значуща позиція одиночного елемента ЦСД відповідає «1», то на РП формується одиночний елемент «1» і навпаки.

Якщо $t_a < T_o$, то говорять, що реєстрація з відсічкою. При інтегральному методі рішення про приймаємий сигнал виноситься в кінці прийому одиночного елемента ЦСД.

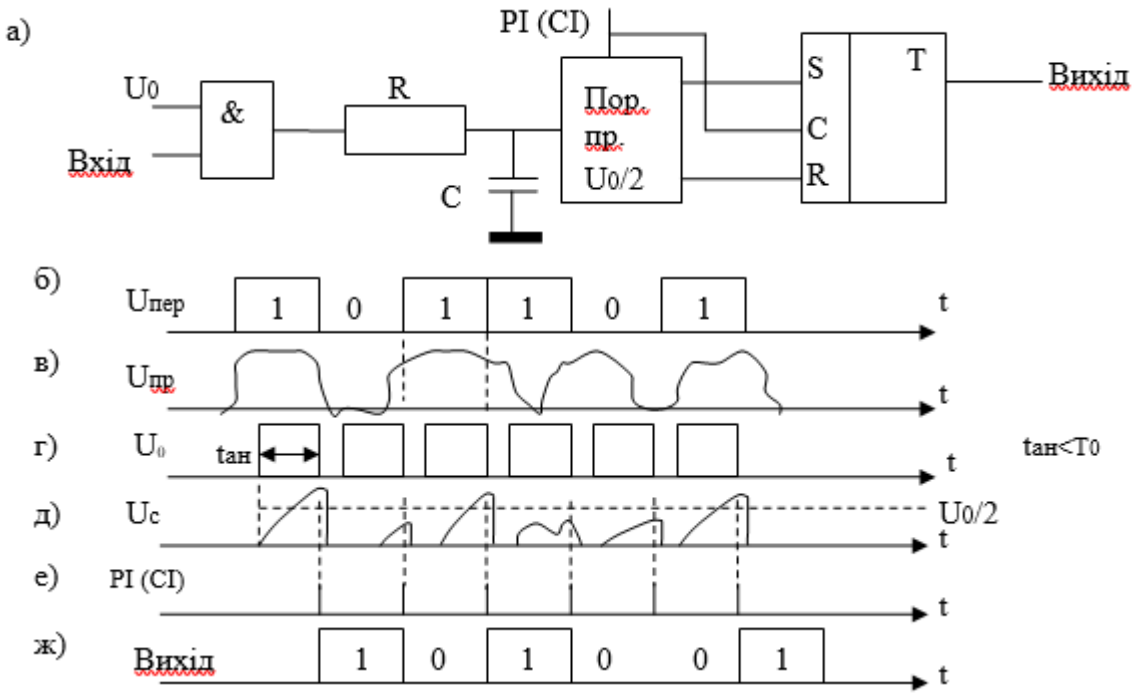


Рисунок 1.12 – Схеми реалізації

У випадку, якщо $t_a = T_o/2$ $\mu_{кр} = \frac{T_o - T_o/2}{2T_o} \times 100\% = 25\%$. Якщо $t_a \Rightarrow 0$, то $\mu_{кр} \Rightarrow 50\%$, як і при методі стробування.

Виправляюча спроможність РП при дробленнях залежить від довжини часу реєстрації і моменту початку дроблень:

$$\mu_{др} = \frac{t_a/2}{T_o} \times 100\% \text{ якщо } t_a \to T_o, \text{ то } \mu_{др} \Rightarrow 50\%$$

$$t_a \to 0, \text{ то } \mu_{др} \Rightarrow 0$$

Реєстрація інтегральним (дискретним) методом

На вхід схеми співпадіння &1 наступають одиничні елементи приймаємого ЦСД і стробуючі імпульси (рисунок 1.13).

Лічильник СТ на $\frac{\varepsilon+1}{2}$ імпульсів відлічує дане число імпульсів на виході &1 і подає на вхід тригеру Т сигнал, що переключає тригер Т. вихідний тригер становиться в стоп, відповідаючи значенню переданого сигналу. Цей же імпульс встановлює лічильник в початковий стан «0». Імпульс з лічильника СТ забороняє проходження стробуючих імпульсів на вхід лічильника.

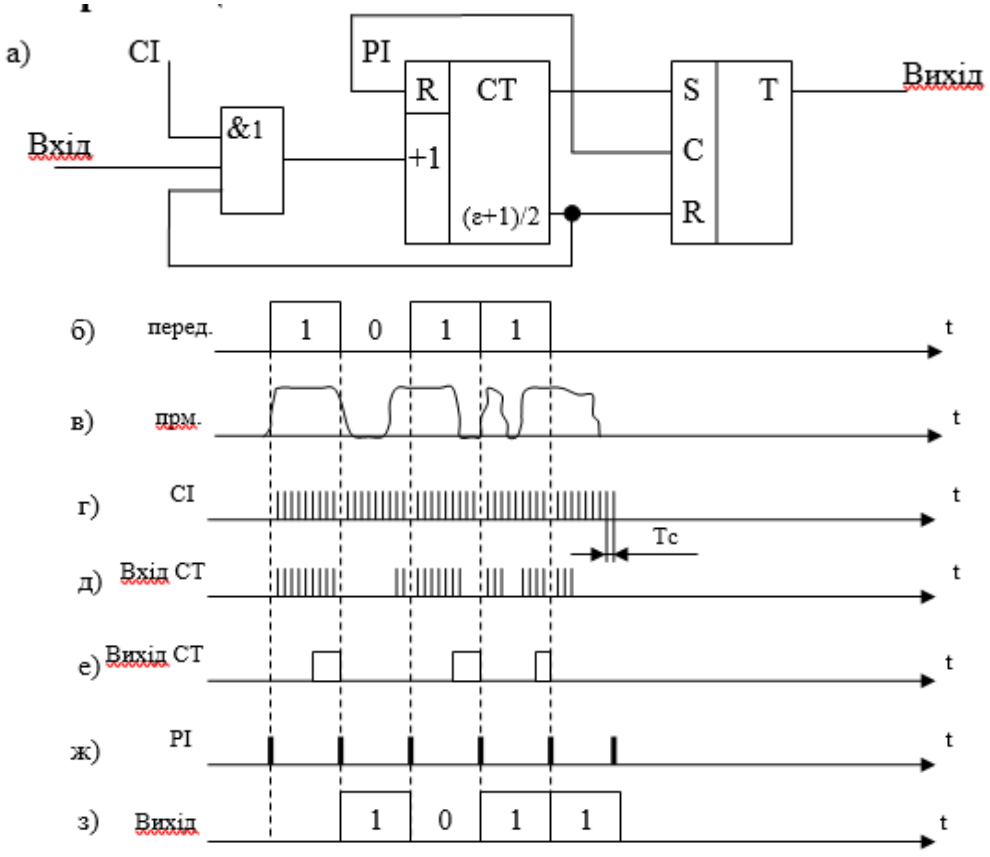


Рисунок 1.13 – Схема реалізації

$t_c = \frac{t_a}{\varepsilon}$ - на інтервалі аналізу стробується в ε - точках (рисунок 1.14).

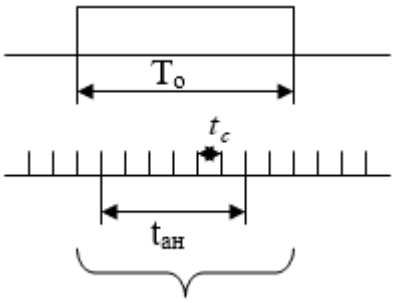


Рисунок 1.14 – Стробування на інтервалі аналізу

На рисунку бачимо, що елемент буде зареєстрованим правильно, якщо непошкоджена частина інтервалу аналізу складає половину від всіх стробів.

$$\frac{\varepsilon-1}{2}\times t_c = \frac{\varepsilon-1}{2}\times\frac{t_a}{\varepsilon}$$

$$\mu_{кр} = \frac{T_o - \frac{\varepsilon-1}{2}\times\frac{t_a}{\varepsilon}}{2T_o}\times 100\% \rightarrow \mu_{кр} = \left(1-\frac{\varepsilon-1}{2}\times\frac{t_a}{\varepsilon T_o}\right)\times 50\%$$

Якщо $t_{ан} = T_o$, то $\mu_{кр} = \left(1+\frac{1}{\varepsilon}\right)\times 25\%$, якщо $\xi \rightarrow \infty$, то $\mu_{кр} = 25\%$.

ЛЕКЦІЯ 3
МЕТОДИ ТА ПРИСТРОЇ СИСТЕМ СИНХРОНІЗАЦІЇ

3.1. Завдання та класифікація систем поелементної синхронізації

Відомо, що при реєстрації дискретних сигналів (одиночних елементів ЦСД), в приймачах необхідно мати строго визначене фазове співвідношення із одиничним інтервалом, на якому здійснюється прийом сигналу.

При **стробуванні** – це середина прийому одиничного елементу, а при **інтегральному** методі – це його кінець.

Отже необхідно встановити і підтримувати ці співвідношення в процесі передачі ДС документального електрозв'язку.

Складність полягає не тільки в тому, що задаючі генератори передавальної та приймальної частин мають нестабільні характеристики, а також з тим, що в каналах діють завади, які викликають певні пошкодження сигналів.

Крім того є завдання, виділення з послідовності прийнятих елементів кодових комбінацій, отже потрібно знати – де їх початок та завершення.

Поелементна (тактова) синхронізація – процес встановлення і підтримки потрібних фазових співвідношень між значимими моментами переданих і прийнятих одиничних елементів ЦСД.

Циклова (групова) синхронізація – процес визначення порядку відліку одиночних елементів ЦСД у груповому сигналі.

Принцип дії пристроїв поелементної синхронізації оснований на аналізі сигналів, що надходять на вхід приймача і формуванні послідовності регіструючих (тактових) імпульсів.

Інформацію про положення значущих моментів передаваємих сигналів можна отримати із інформаційних (робочих) сигналів, що передаються по каналу зв'язку, або за рахунок спеціальних сигналів, передаваємих сумісно із інформаційними чи окремо по спеціальному каналу синхронізації (пілот-сигнал).

Систему поелементної синхронізації по способу передачі інформації розрізняють:

1. Системи з використанням **високостабільних ЗГ** (рисунок 1.15) на ПЕР і ПРМ (системи *без зворотного зв'язку*)

Рисунок 1.15 – Система з використанням високостабільних ЗГ на ПЕР і ПРМ

Розрахунки показують, що в цьому випадку для забезпечення синхронної роботи, наприклад при швидкості цифрового сигналу 2048 кбіт/с необхідно мати ЗГ із відносною нестабільністю $\delta_Г = \frac{\Delta f}{f_{НЗГ}} = 10^{-11}...10^{-12}$, що практично неможливо реалізувати для сучасних систем зв'язку.

2. Системи з використанням **обладнання тактової синхронізації** (рисунок 1.16) ПЕР і ПРМ частин ЦСП (тобто ПРМ частина керується сигналами тактової синхронізації, переданими з ПЕР) – *замкнуті системи*.

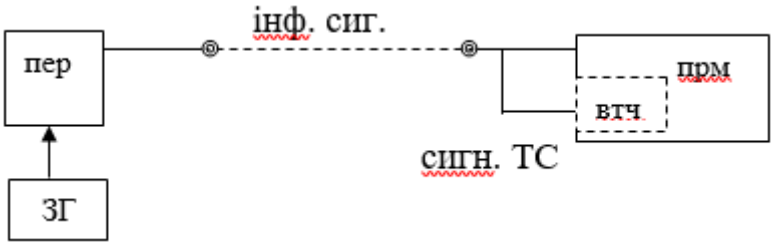


Рисунок 1.16 – Системи з використанням обладнання тактової синхронізації ПЕР і ПРМ

Сигнали тактової синхронізації виділяються на ПРМ спеціальним пристроєм, який називається ВТЧ (видільник тактової частоти)**.** Ці пристрої в ПРМ частині ЦСП виконують роль ЗГ. Це дозволяє використовувати ЗГ на ПЕР із практично реалізуємою нестабільністю $\delta_Г = 10^{-6}.. 10^{-7}$.

У залежності від способу взаємодії ПЕР і ПРМ частин ЦСП, розрізняють такі системи тактової синхронізації:

а) *з передачею спеціального сигналу тактової синхронізації*

У цьому випадку для нього організується або окремий фізичний ланцюг, або окремий канал передачі.

б) *з виділенням сигналу тактової синхронізації з інформаційного сигналу*

У цьому випадку сигнал ТС виділяється певним чином безпосередньо з інформаційного сигналу.

3.2. Принципи роботи системи поелементної синхронізації

При значних відстанях між АПД доцільним є використання систем з виділенням сигналу ТС з інформаційного сигналу.

Відомі такі способи виділення сигналу ТС з інформаційного:

а) на основі **пасивної** фільтрації за допомогою вузькосмугових ПФ (безпосередньо зі спектра інформаційного сигналу);

б) на основі **автопідстроювання** частоти ЗГ прийомної частини ЦСП:

– з аналоговим керуванням;
– з дискретним керуванням.

1. Ідея побудови **системи ПЕС із пасивною фільтрацією** полягає у

виділенні за допомогою вузькосмугового ПФ зі спектра інформаційного сигналу коливання тактової частоти f_T.

Функціональна схема ВТЧ, побудованого на основі цього методу і часові діаграми, що пояснюють його роботу приведені на рисунку 1.17.

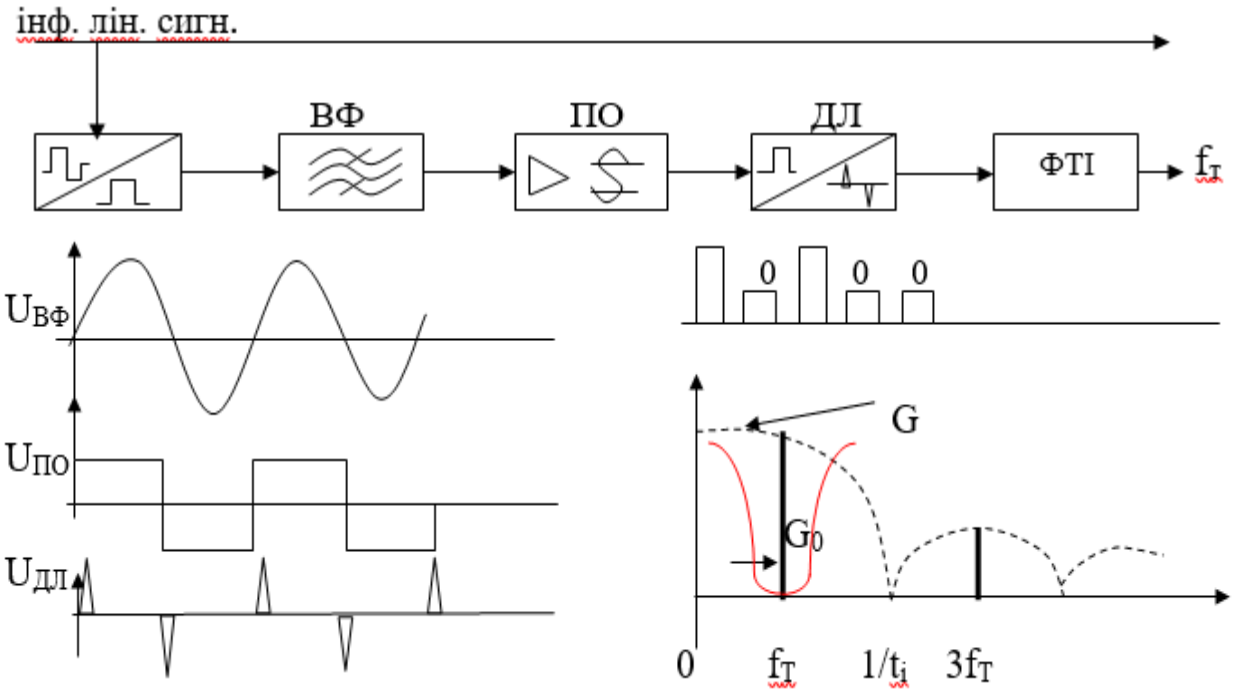


Рисунок 1.17 – Функціональна схема ВТЧ та часові діаграми системи ПЕС із пасивною фільтрацією

Виділення коливання актової частоти можливо тільки з одно полярної послідовності інформаційного сигналу. Якщо вона двохполярна (у неї в спектрі немає $f_т$), то необхідно перетворити її в однополярну.

Відомо, що енергетичний спектр випадкової послідовності однополярних імпульсів (інформаційний сигнал) містить як безперервну $G_Б(t)$, так і дискретну складові $G_д(t)$. Дискретна частина енергетичного спектра являє собою гармоніки, кратні тактовій частоті.

За допомогою вузькосмугового фільтру (ВФ) зі спектра інформаційного сигналу виділяється перша гармоніка дискретної складової спектра з частотою рівної $f_{т\ інф.сиг}$

Гармонійне коливання з тактовою частотою $f_{т\ інф.сиг}$ перетворюється за допомогою ДЛ (диференціруючого ланцюга) у послідовність коротких імпульсів.

У ФТІ (формувачі тактових імпульсів) послідовність коротких імпульсів із ДЛ перетворюється в послідовність стробуючих імпульсів, слідуючих з тактовою частотою:

$$f_т=f_{т\ інф.сиг}=1/T$$

Переваги схеми:

– простота реалізації;

– немає необхідності мати для забезпечення її роботи опорне коливання (допоміжне) від ГО (тобто таку схему можна використовувати в тих елементах ЦСП, де немає власного ГО, наприклад, необслуговуємі регенератори).

Розглянута схема має деякі недоліки:

– Коливання тактової частоти на виході ВТЧ пропадає при пропаданні інформаційного сигналу.

– З появою в інформаційному сигналі довгої послідовності "0" (що аналогічно відсутності інформаційного сигналу) коливання тактової частоти на виході ВТЧ буде відсутнє. Отже, ВТЧ працює хитливо (при пачці "0" можливі пропадання коливання тактової частоти).

2. **Система поелементної синхронізації (ПЕС) із фазовим автопідстроюванням частоти**

Ідея роботи СПЕС з автопідстроюванням частоти полягає в тому, що з інформаційного сигналу виділяється не власне тактова частота, а інформація про відмінність його тактової частоти від місцевого ГТЧ (опорної частоти). Далі ця інформація використовуються для доведення частоти місцевого ГТЧ до величини, що відповідає тактовій частоті інформаційного сигналу.

В залежності від способу керування зміною частоти місцевого ГТЧ розрізняють схеми ВТЧ із:

– аналоговим керуванням фазовою автопідстройкою частоти (АФАПЧ);

– дискретним керуванням фазовою автопідстройкою частоти (ДФАПЧ), або так ще називають "дискретне автопідстроювання фази" (ДАПФ).

Структурна схема ВТЧ з **АФАПЧ** приведена на рисунку 1.18.

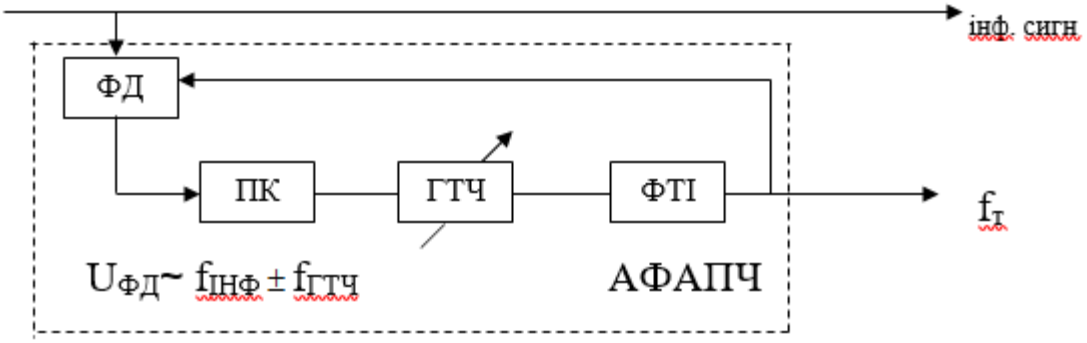


Рисунок 1.18 – Структурна схема ВТЧ з АФАПЧ

В якості джерела опорної частоти використовується перебудовуємий ГТЧ, що формує гармонійний (аналоговий) сигнал.

На один вхід фазового детектора (ФД) надходить інформаційний сигнал. Цей сигнал є вхідним для ВТЧ. Вихідним сигналом ВТЧ є послідовність імпульсів слідуючих з тактовою частотою $f_т$.

По петлі зворотного зв'язку сигнал тактової частоти надходить також

на другий вхід ФД

ФД визначає зсуви фаз (розходження довжини імпульсів) між двома послідовностями імпульсів.

У первісний момент часу при різниці тактових частот інформаційного сигналу і місцевого ГТЧ на виході ФД буде сигнал про їх фазовий зсув. Надалі за допомогою сигналу фазового зсуву через пристрій керування ПК здійснюється **зміна** частоти ГТЧ доти, поки фазовий зсув не буде мінімізований, тобто тактові частоти ГТЧ і інформаційного сигналу будуть рівні:

$$f_{інф} = f_т$$

Структурна схема ВТЧ із ДФАПЧ приведена на рис. 2.3. В якості опорної частоти використовується дискретна послідовність імпульсів від генераторного устаткування ГО, слідуючих з частотою:

$$n \bullet f_г = n \bullet f_Т.$$

Як і в схемі АФАПЧ ФД визначає фазовий зсув між послідовностями імпульсів вхідного сигналу (інформаційного) і вихідного (тактової частоти), що надходить на ФД по ланцюзі зворотного зв'язку (петля ДАПФ).

В залежності від знака зрушення фаз по сигналу з ФД в ПК здійснюється або виключення, або вставляння імпульсів у сигнал опорної частоти з метою мінімізації фазового зрушення (рисунок 1.19). У результаті вихідним сигналом ВТЧ є послідовність імпульсів, слідуча з частотою, близькою до тактової частоти інформаційного сигналу.

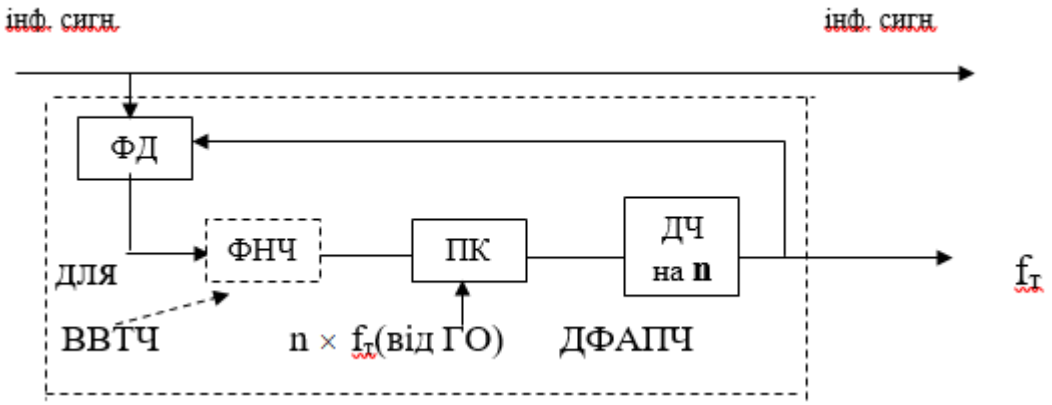


Рисунок 1.19 – Мінімізації фазового зрушення

Проведення операції виключення і вставляння імпульсів у високій області частот з наступним діленням у ДЧ дозволяє зменшити виникаючий у вихідному сигналі ефект тремтіння фази.

3.3. Принципи роботи системи циклової синхронізації

Рівність швидкостей обробки сигналів у всіх елементах СПД, забезпечується тактовою синхронізацією, вона є необхідною умовою нормальної роботи СПД, але недостатньою.

Для правильного функціонування ЦСП необхідно виконувати також умови синфазності (одночасності) роботи передавальної і приймальної частин ЦСП. Це досягається за допомогою системи циклової синхронізації.

Розглянемо загальну ідею роботи системи циклової синхронізації/

На передачі в пристрої часового об'єднання (ПЧО) формується цифровий сигнал передачі (ЦСпер). З метою забезпечення синфазної роботи ПЕР і ПРМ частин СПД у ЦСпер від циклового розподільника передачі (ЦР1) вводиться спеціальний синхросигнал**,** що являє собою групу імпульсів визначеної комбінації. Так як синхросигнал вводиться від ЦР1 з визначеною періодичністю, то і ЦСпер буде являти собою циклічну структуру, де початок (кінець) кожного циклу визначається синхрогрупою.

Синхросигнал має бути:

– Як можливо коротшим, щоб не займати пропускну здатність каналу та швидче забезпечувати входження в синхронізм.

– Забезпечувати мінімальну ймовірність збігання із інформаційними символами (тобто досить довгим).

– Регулярним.

Відповідно до алгоритму роботи ЦР1 кожна позиція циклу має своє призначення (тобто несе інформацію про 1-ший КС, 2-гій КС, про синхросигнал і т.д.).

На прийомі ЦСпер надходить на пристрій часового розподілу (ПЧР), де позиції треба визначити позиції 1 КС, позиції 2-го КС і т.д. З цією метою і працює система циклової синхронізації.

Основний елемент системи циклової синхронізації на ПРМ – **приймач синхросигналу**, що і забезпечує синфазну роботу ПЕР і ПРМ частин СПД. У найпростішому випадку приймач складається з опізнавача й аналізатора (рисунок 1.20).

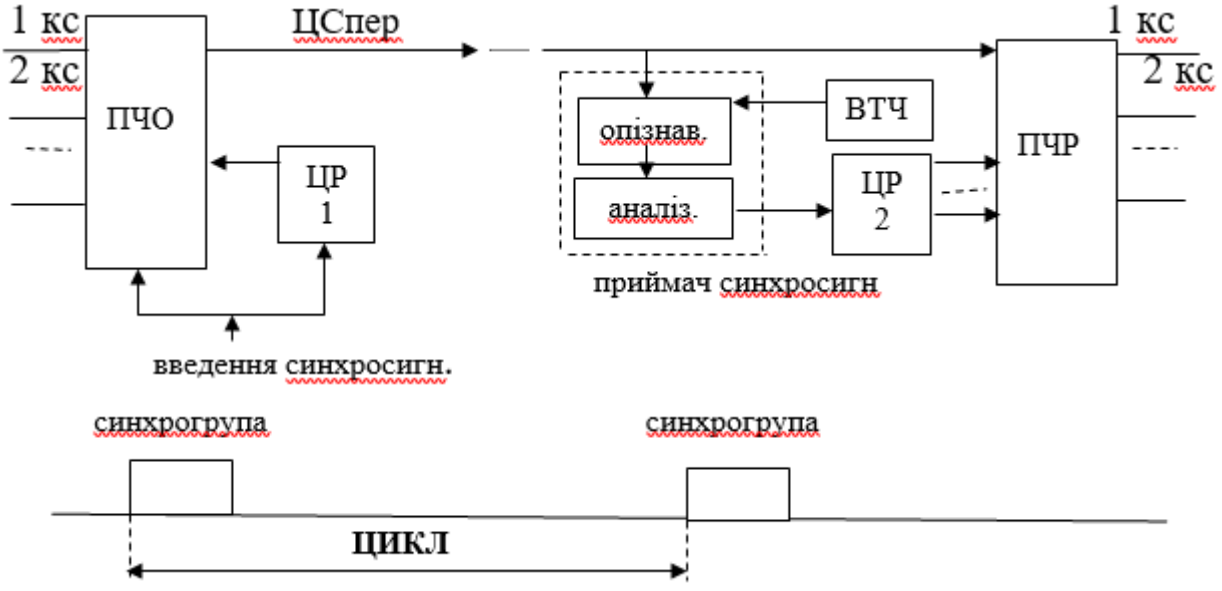


Рисунок 1.20 – Система циклової синхронізації на ПРМ

Опізнавач призначений для виділення з ГЦС кодових комбінацій, що збігаються за структурою з синхросигналом. Сигнал на виході опізнавача буде тільки в тому випадку, якщо на його вхід надійшла кодова комбінація, що збігається за структурою із синхросигналом.

Аналізатор визначає відповідність часу приходу синхрогрупи з ПЕР частині і часу формування синхрогрупи в цикловому розподільнику ПРМ частини (ЦР2). Якщо час приходу і час формування збігаються, то значить робота ПЕР і ПРМ частин синфазна**.** У такому випадку аналізатор дає команду на дозвіл ЦРпрм розподілити в ПЧР позиції ЦСпер, які надходять на його вхід. Такий режим роботи СПД називають робочим режимом або *станом синхронізму*. У цьому випадку ПРМ-синхросигнала здійснює контроль за станом синхронізму в робочому режимі (утримує синхронізм).

Якщо час приходу і час формування не збігаються, то значить немає синфазної роботи ПЕР і ПРМ частин. У такому випадку аналізатор дає команду заборони ЦР2 на розподіл в ПЧР позицій ЦСпер. Такий режим роботи ЦСП називають станом порушення синхронізму. У цьому випадку ПРМ-синхросигнала повинний здійснювати відновлення синхронізму, тобто працювати в режимі пошуку синхросигнала.

Всього можливі наступні стани системи циклової синхронізації (рисунок 1.21):

- I – режим синхронізму
- II – режим перевірки за виходом із синхронізму
- III – режим пошуку синхронізму
- IV – режим перевірки за входом у синхронізм
- V – стан переходу в помилковий синхронізм

Вони співвідносяться за такою блок-схемою

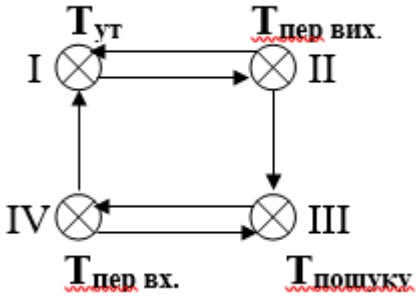


Рисунок 1.21 – Блок-схема станів системи циклової синхронізації

Режими II та IV введені з метою запобігання помилкового прийому (або помилкового не прийому) синхрогрупи. Щоб не було помилкового збою циклового синхронізму при перекручуванні тільки одної синхрогрупи вводять режим II - перевірки за виходом із синхронізму, у ході якого робиться упізнання синхрогрупи в наступному циклі і т.д. Якщо підряд буде перекручено N-синхрогруп, то тільки тоді приймається рішення про перехід у режим пошуку III. З цією метою до складу опізнавача вводять накопичувач

(рисунок 1.22).

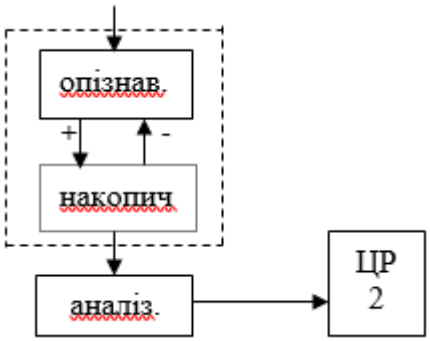


Рисунок 1.22 – Схема введення накопичувача до складу опізнавача

Накопичувач підсумовує результати упізнання N-синхрогруп. На підсумовуючий вхід накопичувача надходять сигнали з опізнавача при упізнанні синхрогрупи. Накопичувач складає ці сигнали і по його заповненні дає команду – дозвіл на запуск ЦР2.

Якщо немає упізнання однієї або декількох синхрогруп, то сигнал з виходу опізнавача надходить на вхід накопичувача, що віднімає. Команда на зупинку ЦР2 може з'явитися тільки при повному спустошенні накопичувача (при неупізнанні підряд N-синхрогруп).

При помилковому збої синхронізму (перекручені тільки синхрогрупи, причому в кількості меншій N) накопичувач не спустошується й у результаті не дає команду на зупинку ЦР2, а ПЕР і ПРМ частини продовжують працювати в синхронному режимі.

Таким чином, окремі збої (перекручування) синхрогруп не приведуть до втрати синхронізму.

ЛЕКЦІЯ 4
ПРИНЦИПИ ФАКСИМІЛЬНОЇ ПЕРЕДАЧІ ПОВІДОМЛЕНЬ

4.1. Характеристика та особливості реалізації факсимільного зв'язку

Факсимільний зв'язок – це вид документального електрозв'язку, який забезпечує передачу нерухомих зображень по каналах зв'язку (тексту, малюнків, таблиць, графіків, фотографій) з відтворенням на паперовому носії.

Переваги факсимільного зв'язку:

– можливість передачі практично будь-якого зображення нанесеного на папір: літерно-цифрове, телеграфне, креслення, рукописне, картографічне і т.і.

– висока завадостійкість, завдяки високій надмірності зображень.

– виключається участь людини (оператора) в процесі передачі і прийому, тобто висока ступінь автоматизації.

Недоліки факсимільного зв'язку:

– велика надмірність зображень суттєво зменшує швидкість передачі;

– потрібно відносно широку смугу частот для передачі зображення.

Класифікація факсимільної апаратури (ФА):

І. МСЕ-Т розподіляє факсимільну апаратуру (ФА) *за призначенням* на два класи:

1) ФА загального призначення (для передачі ділової інформації – текстових і графічних матеріалів);

2) ФА спеціального призначення (для передачі газетних смуг, фотографічних матеріалів, метеорологічних карт, для забезпечення пере приймання в проміжному пункті факсимільної інформації в цифровій формі).

ІІ. Факсимільна апаратура загального призначення розподіляється МСЕ-Т на *4 групи*:

1) апаратура, яка забезпечує передачу сторінки формату А4 по каналах ТЧ з розрізняльною здатністю 3,85 лін/мм за час до 6 хвилин.

2) Апаратура, яка забезпечує передачу за таких же умов за 3 хвилини.

3) Апаратура в якій використовуються цифрові методи подання, опрацювання і передачі сигналів, реалізовані методи стискання інформації, а час передачі не перевищує 1 хвилини і залежить від степені стиснення, розрізняльна здатність 2,57; 3,85; 7,7 лін/мм, передбачається передача по КТЧ.

4) Апаратура, в якій розширені можливості апаратури 3 групи, для передачі використовується, крім каналу тональної частоти (КТЧ), також канали ПД і передбачається можливість варіацій способів передачі документа в залежності від особливостей його побудови.

III. В залежності від кольору оригінала, який передається і копії (репродукції), яка прийнята факсимільні апарати розподіляються:

1) для передачі і прийняття чорно-білих зображень;

2) для передачі кольорових зображень і приймання їх у вигляді чорно-білих зображень з різними градаціями відтінків;

3) передача і приймання кольорових зображень.

Особливості реалізації факсимільного зв'язку:

– Необхідність оптичного аналізу зображення, яке передається (оригінал) і пов'язані з цим особливості побудови аналізуючого пристрою.

– Перетворення світлового потоку в електричний сигнал і пов'язані з цим принципи побудови фотоелектричного перетворювача (ФЕП).

– Надзвичайно висока надмірність інформації в зображенні в порівнянні з іншими видами електрозв'язку, і пов'язана з цим необхідність використання високоефективних методів стискання інформації.

– Розщеплення світлового потоку на три складові (R, G, B) при опрацюванні кольорових зображень і використання трьох однакових трактів перетворення отриманих сигналів в апаратурі та використання спеціального алгоритму передачі по каналам зв'язку.

– Перетворення прийнятих сигналів на приймальній стороні у відповідності з алгоритмом, який забезпечує синтез (відтворення) зображення.

– Синтез зображення (створення репродукції) на фізичному носії (спеціальний папір, звичайний папір, фотопапір).

– Великий обсяг математичних обчислень на ПРД і ПРМ при опрацюванні кольорових зображень, що вимагає використання процесорів з високою продуктивністю і великим об'ємом пам'яті.

Слід зазначити, що для передачі чорно-білих і кольорових зображень можна використати сучасні комп'ютерні технології: на передавальній стороні – сканер для аналізу зображення, а на приймальній стороні – принтер для синтезу (відтворення) зображення. До речі принципи побудови і технології сканерів і принтерів зародились в області факсимільного зв'язку – ще одне підтвердження інтеграційних процесів у системах телекомунікацій. Але використання такого симбіозу (сканер – ПК – лінія зв'язку – ПК – принтер) дорожче, ніж двох ФСА, з'єднаних каналом зв'язку, тому роботи по вдосконаленню ФСА продовжуються і сьогодні.

4.2. Структурна схема факсимільної системи

Принципи передачі і прийому зображення ілюструються на рисунку 1.23.

Зображення розбивається на рядки відстань між серединами яких (крок) складає величину δ, а кожний рядок розбивається на окремі елементарні площадки $\rho(x, y)$, які називаються растр-елементами (пікселями). Стандартом МСЕ-Т визначається кількість растр-елементів (пікселів) для ФСА групи 3 в одному рядку – 1728, тобто 8 точок на 1 мм

зображення при довжині рядка 216 мм формату А4. По вертикалі розрізнюваність складає 7,7 лін/мм.

Яскравість растр-елемента в його межах практично однакова і залежить від зображення, мікрочастину якого відтворює даний растр-елемент. Растр-елемент послідовно по рядку і по кадру злічується розгортаючим пристроєм, їх світлова інтенсивність перетворюється в електричні сигнали $U_c(t)$, опрацьовується передавачем (перетворюється в цифрову форму, стискається, модулюється) і передається по каналу зв'язку у вигляді сигналу $U(t)'$.

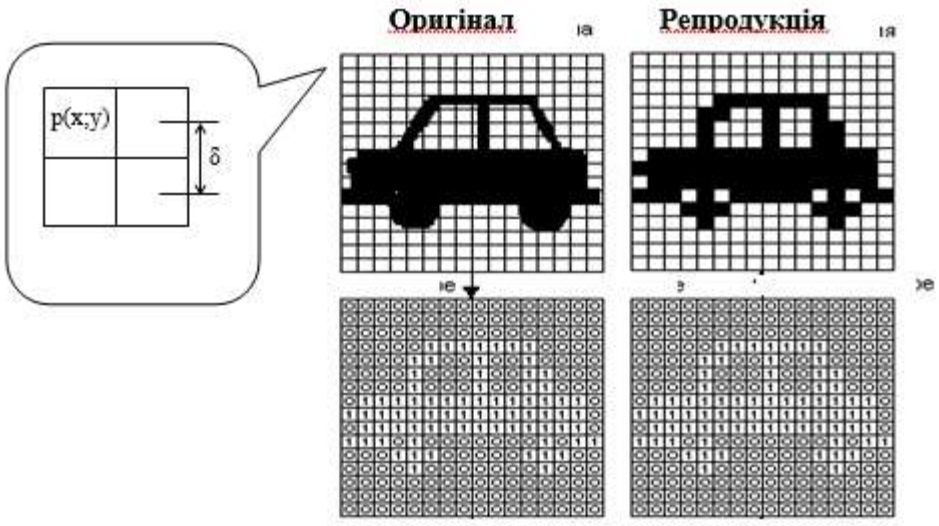


Рисунок 1.23 – Принцип передачі і прийому зображень

На приймальній стороні в результаті опрацювання прийнятого сигналу $U'(t)$ в електричному тракті приймача відтворюється з певною точністю сигнал $U_c'(t)$, за допомогою якого синтезуючий пристрій формує растр-елемент $\rho'(x', y')$ і зображення в цілому.

Зображення, яке передається називається оригіналом, а яке відтворюється – **репродукцією**.

Структурна схема факсимільної системи представлена на рисунку 1.24

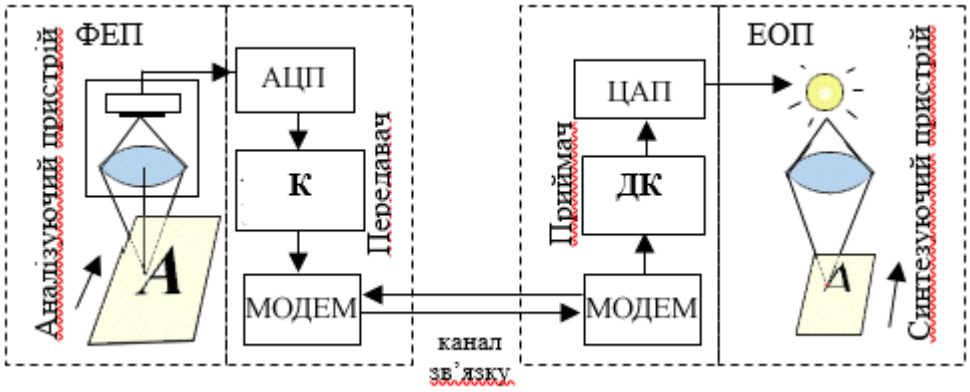


Рисунок 1.24 – Структурна схема факсимільної системи

Схема складається із:

– аналізуючого пристрою;
– електричного тракту передавача;
– каналу зв’язку;
– електричного тракту приймача;
– синтезуючого пристрою.

Для забезпечення синхронного і синфазного пересування пристроїв розгортки на передавальній і приймальній сторонах використовуються пристрої синхронізації і фазування.

Синхронізація забезпечує рівномірність розгортки вздовж рядка (на передачі – це зчитування растр-елементів вздовж рядка, а на прийманні – це їх синтез вздовж рядка).

Бланки оригіналу та репродукції можуть закріплюватись на барабанах, які крутяться синфазно і синхронно, або протягують через пристрої з плоскими поверхнями. Останній спосіб набув найбільшого розповсюдження.

За допомогою сфокусованого в точку (або в лінію рядка) (рисунок 1.25) променя використовується зчитування растр-елементів вздовж рядка.

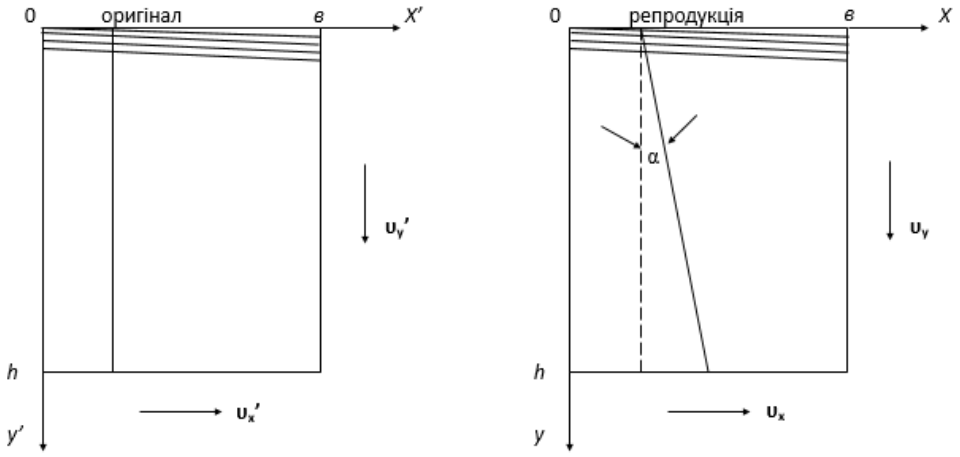


Рисунок 1.25 – Приклад зчитування растр-елементів

Відбитий від растр-елемента промінь падає на фотоелементи (фотоелектричного перетворення – ФЕП) і викликає на його виході електричний сигнал $U_c(t)$, який пропорційний яскравості растр-елементу (оптичній щільності зображення $\rho(x, y)$).

В електричному тракті передавача виконується підсилення та модуляція сигналу, використовується АМ, ЧМ, ВФМ та більш складні методи модуляції (АФМ, КАМ, багатомірна КАМ).

В електричному тракті приймача використовується зворотнє перетворення сигналу до значень, які потрібні для стандартизованого записування (відтворення) зображення.

Для синтезу зображення використовуються наступні носії репродукції:

– звичайний папір;
– спеціальний папір (електрохімічний, електростатичний, термохімічний та ін.);

– фотопапір.

–

4.3. Основні параметри факсимільної апаратури

До основних параметрів факсимільної апаратури відносять:

1) крок розгортки δ - це відстань між серединами двох сусідніх рядків. $0{,}92 \le \frac{\delta}{d_{\min}} \le 1$, тут $d_{\min}$ - мінімальний розмір деталі, яку треба відтворити. Для машинописних текстів $d_{\min} = 0{,}35мм$, для інших 0,1 – 0,25.

2) Форма і розміри растр-елемента (рисунок 1.26):

Рисунок 1.26 – Форма растр-елемента

3) довжина рядка розгортки В. У звичайних ФСА В=220 мм, у ФСА для передачі метеокарт В=440 мм, у спеціальних кольорових системах („Цвет”) В=900.

4) Розрізняльна здатність ФСА – це здатність розрізняти і відтворювати дрібні деталі зображення. Визначається розміром растр-елемента.

5) Швидкість розгортки (передачі). Швидкість розгортки визначається кількістю рядків які опрацьовуються за 1 хв.

6) Щільність розгортки ФСА – це кількість ліній на 1 мм зображення. Використовується поняття густини по вертикалі $n_{верт}$ і горизонталі $n_{гор}$:

$$n_{верт} = \frac{1}{\delta};\ n_{гор} = \frac{1}{a_p}$$

Для цифрових ФСА ця величина визначається кількістю точок на 1 мм. У ФСА 3 групи – це 8 точок по горизонталі і 7,7 по вертикалі.

Добре відтворення напівтонових і штрихових зображень досягається при густині розгортки 6-7 лін/мм.

Для задовільного відтворення рукописних матеріалів та мапи – рукописного тексту достатньо 4-5 лін/мм.

Для передачі газет використовується 1,54 лін/мм і більше.

7) модуль взаємодії М – це відношення довжини рядка В до кроку розгортки δ:

$$M = \frac{B}{\delta \cdot \pi},$$

рівність модулів розгортки визначає можливість обміну між двома ФСА без геометричних спотворень. Стандартні значення М=264, 352 та ін.

8) смуга частот ФСА. Спектр частот факсимільного сигналу займає від частин Герц до десятків кГц. Структура його залежить від характеру зображень.

4.4. Стиснення даних

Для зменшення смуги частот потрібної для передачі ФСА застосовують **стиснення даних** (зменшення надмірності). Розрізняють стискання даних *без втрат*, тобто коли закодовані дані однозначно можуть бути відновлені з точністю до біта, та *з втратами*, коли розпаковані дані відрізняються від вихідних, але ступінь відмінності не є істотним з погляду їх подальшого використання.

Другій тип компресії часто застосовується для стиску аудио-(mpeg3) і відеоданих (mpeg4), статичних зображень (jpeg), і цифрової телефонії (вокодер).

А в ФСА знайшли застосування методи стискання без втрат. Деякі з них:

Алгоритм RLE (Run Lengh Encoding – кодування довгих серій КДС) – один із самих старих і самих простих алгоритмів архівації графіки.

Само стиснення здійснюється за рахунок того, що в початковому зображені зустрічаються послідовності однакових бітів (байтів). Їх можна замінити на пару лічильних повторів – значення, що зменшує надмірність. Існує три модифікації – КДС-1, КДС-2, КДС-3

Найбільш простим серед КДС є КДС-1. Сигнал від кожної строчки розгортання передаваємого зображення розбивається на окремі елементи – дискретизується. Елементам білого присвоюється значення „0”, а чорного – „1”. Кодування здійснюється групами. Групи, що містять переходи від білого до чорного, або чорного до білого не кодуються – передаються в **незмінному вигляді.**

Групи, що містять одні „0” і групи, що містять одні „1” кодуються двійковими числами, які показують кількість груп одного кольору, що ідуть підряд.

Якщо число груп кодується двійковими чотирирозрядними числами (4 розряди). Кодова комбінація на виході крім цих 4-х розрядів містить старші два розряди 5 і 6, що визначають характер комбінації (рисунок 1.27):

– **10** – кодова комбінація, містить некодуєму групу (групи 1, 2, 18);

– **01** – число послідовних груп чорного (чотири молодших розряди – вкаже число груп);

– **00** – число послідовних груп білого;

– **11** – комбінація містить сигнал управління (синхронізація – 11000 перед кожною строчкою).

Таким чином, можна закодувати 15 груп „однокольорових”, тобто 01 (чорних), 00 (білих).

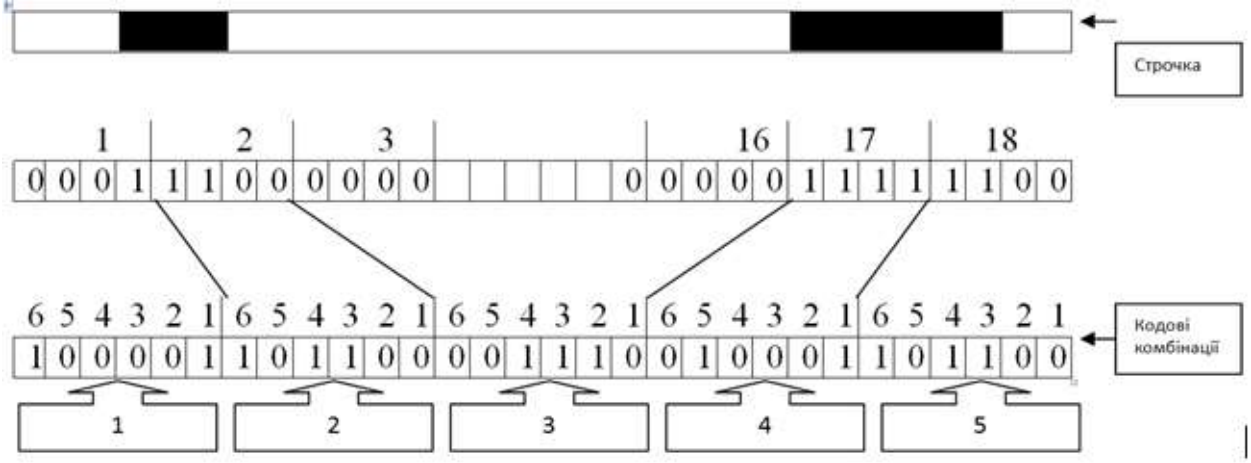


Рисунок 1.27 – Кодова комбінація

Ефективність стиснення можна оцінити коефіцієнтом стиснення $К_{ст}$. В наведеному прикладі, для передачі 72 елементів розкладу строчки 4×18=72 буде передано 5 кодових комбінацій по 6 елементів = 30.

$$К_{ст} = 72/30 \approx 2$$

Алгоритм Хафмана – адаптивний простий алгоритм оптимального префіксного кодування алфавіту з мінімальною **надмірністю**.

Цей метод кодування складається із двох основних етапів:

– Побудова оптимального кодового дерева.

– Побудова відображення код-символ на основі побудованого дерева.

Ідея алгоритму полягає в наступному: знаючи ймовірності символів у повідомленні, можна описати процедуру побудови кодів змінної довжини, що полягають із цілої кількості бітів. Символам з більшою ймовірністю ставляться у відповідність більш короткі коди. Коди Хафмана мають властивість **префіксності** (т.т. жодне кодове слово не є префіксом іншого), що дозволяє однозначно їх декодувати.

Класичний алгоритм Хафмана на вході одержує таблицю частот використання символів у повідомленні. Далі на підставі цієї таблиці будується дерево кодування Хафмана (Н-дерево).

Алгоритм:

1. Символи вхідного алфавіту утворюють список вільних вузлів. Кожний пункт має вагу, яка може бути рівною або ймовірності, або кількості входжень символу в повідомлення.
2. Вибираються два вільні вузли дерева з найменшими вагами.
3. Створюється їхній „батько” з вагою, рівною їх сумарній вазі.
4. „Батько” додається в список вільних вузлів, а два його нащадки видаляються із цього списку.
5. Однієї дузі, що виходить із „батька”, ставиться у відповідність біт 1, іншої – біт 0.

6. Кроки, починаючи із другого, повторюються доти, поки в списку вільних вузлів не залишиться тільки один вільний вузол. Він і буде вважатися коренем дерева.

Візьмемо для прикладу набір символів:

11111111111111111111111122222233333444445555666677 88,

у якому є 8 видів символів (тобто для їхньої передачі буде потрібно 3-хзначне кодування). Усього в наборі перебувають 52 символу, тобто при звичайному кодуванні довжина повідомлення складе: 52x3=156 біт. Частота повторення символів наведена в таблиці 1.4

Таблиця 1.4

Символ	1	2	3	4	5	6	7	8	∑
Частота	24	6	5	5	4	4	2	2	52

Спочатку по Хафману треба вибрати два символи, найбільш рідкі в тексті, і приписати одному біт =0, а іншому – біт =1. У наслідку ці біти виявляться останніми у представленні цих двох обраних символів. У цьому випадку це "8", їй припишемо 1 і "7", їй припишемо 0.

Далі пропонується замість восьми вихідних символів працювати з початковими: "1", "2", "3", "4", "5", "6" і якимось допоміжним символом "Z" (позначення особливої ролі не відіграє), для якого підсумуються кількості входжень символів "8" і "7". Т.т. далі маємо справу з кількостями, наведеними в таблиці 1.5:

Таблиця 1.5

Символ (код)	1 (–)	2 (–)	3 (–)	4 (–)	5 (–)	6 (–)	7 (0)	8 (1)
							Z (–)	
Частота	24	6	5	5	4	4	4	

У таблиці 1.4 найменш частими символами є символи "5", "6", проробимо аналогічну операцію (результат у таблиці 1.6).

Таблиця 1.6

Символ (код)	1 (–)	2 (–)	3 (–)	4 (–)	5 (0)	6 (1)	7 (0)	8 (1)
					Y (–)		Z (–)	
Частота	24	6	5	5	8		4	

На наступній ітерації об'єднанню підлягають символи "4" і "Z" утворюючи "X" із частотою 9 (таблиця 1.7).

Таблиця 1.7

Символ (код)	1 (–)	2 (–)	3 (–)	4 (0)	7 (0)	8 (1)	5 (0)	6 (1)
					Z (1)		Y (–)	
				X (–)				
Частота	24	6	5	9			8	

Тепер мінімальні значення мають символи "2" і "3", поєднуємо їх у символ "W" із частотою 11 (таблиця 1.8).

Таблиця 1.8

<table>
<tr><td rowspan="3">Символ (код)</td><td rowspan="3">1 (–)</td><td>2 (–)</td><td>3 (–)</td><td rowspan="2">4 (0)</td><td>7 (0)</td><td>8 (1)</td><td>5 (0)</td><td>6 (1)</td></tr>
<tr><td colspan="2" rowspan="2">W (–)</td><td colspan="2">Z (1)</td><td colspan="2" rowspan="2">Y (–)</td></tr>
<tr><td colspan="4">X (–)</td></tr>
<tr><td>Частота</td><td>24</td><td colspan="2">11</td><td colspan="4">9</td><td colspan="2">8</td></tr>
</table>

Далі " X" і " Y" при об'єднанні позначимо символом "V" із частотою 15 (таблиця 1.9).

Таблиця 1.9

<table>
<tr><td rowspan="4">Символ (код)</td><td rowspan="4">1 (–)</td><td>2 (–)</td><td>3 (–)</td><td rowspan="2">4 (0)</td><td>7 (0)</td><td>8 (1)</td><td>5 (0)</td><td>6 (1)</td></tr>
<tr><td colspan="2" rowspan="3">W (–)</td><td colspan="2">Z (1)</td><td colspan="2" rowspan="2">Y (1)</td></tr>
<tr><td colspan="4">X (0)</td></tr>
<tr><td colspan="6">V (–)</td></tr>
<tr><td>Частота</td><td>24</td><td colspan="2">11</td><td colspan="6">17</td></tr>
</table>

Останнє об'єднання застосуємо для символів "V" і "W", утворюючи символ "U" із частотою 28. Після такої операції залишається всього два символи "1" і "U" їм привласнюємо відповідно значення 0 і 1 (таблиця 1.10). Більш наочно даний результат представляється графічно у вигляді дерева (рисунок 1.28).

Таблиця 1.10

<table>
<tr><td rowspan="4">Символ (код)</td><td rowspan="4">1 (0)</td><td>2 (–)</td><td>3 (–)</td><td rowspan="2">4 (0)</td><td>7 (0)</td><td>8 (1)</td><td>5 (0)</td><td>6 (1)</td></tr>
<tr><td colspan="2" rowspan="3">W (–)</td><td colspan="2">Z (1)</td><td colspan="2" rowspan="2">Y (1)</td></tr>
<tr><td colspan="4">X (0)</td></tr>
<tr><td colspan="6">V (–)</td></tr>
<tr><td>Частота</td><td>24</td><td colspan="8">U (1)
28</td></tr>
</table>

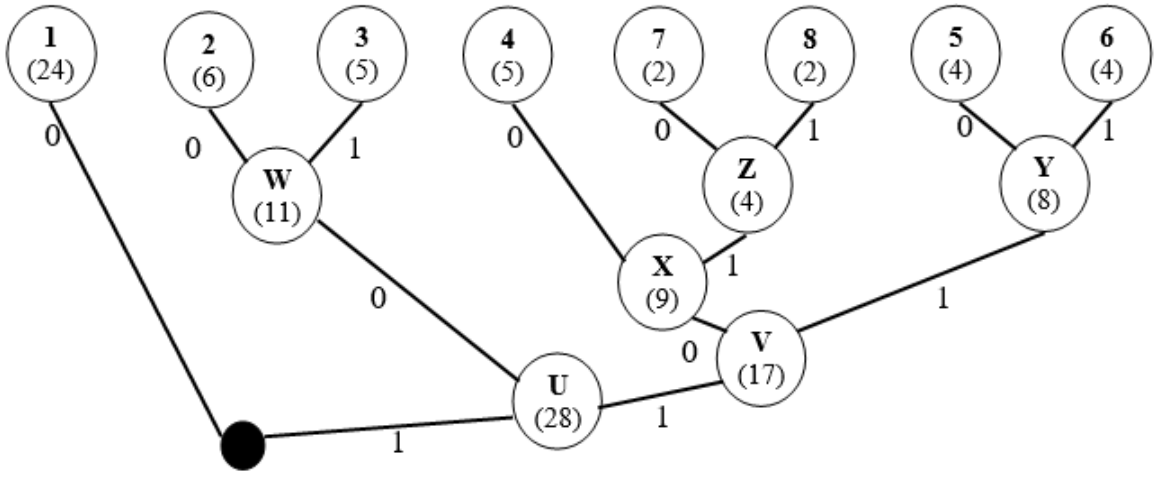


Рисунок 1.28 – Дерево Хаффмана

Вертаючись по побудованому дереву до його початку, збираємо ланцюжки бітів і одержуємо представлення (таблиця 1.11).

Таблиця 1.11

Символ	1	2	3	4	5	6	7	8	∑
Частота	24	6	5	5	4	4	2	2	52
Код	0	100	101	1100	1110	1111	11010	11011	
Кількість біт	24	18	15	20	16	16	10	10	129

У такому випадку вихідний текст можна передати з використанням 129 біт, що на 20% менше від вихідного (156 біт).

Алгори́тм Ле́мпеля-Зіва-Велча (Lempel-Ziv-Welch, LZW) – це універсальний алгоритм стискання даних без втрат.

Даний алгоритм при стисканні (кодуванні) динамічно створює таблицю перетворення рядків: певним послідовностям символів (словам) ставляться у відповідність групи біт фіксованої довжини (звичайно 12-бітні). Таблиця починається всіма 1-символьними рядками (у випадку 5-бітних символів – це 32 записи). У міру кодування, алгоритм переглядає текст символ за символом, і зберігає кожний новий, унікальний 2-символьний рядок у таблицю у вигляді пари код/символ, де код посилається на відповідний перший символ. Після того як новий 2-символьний рядок збережений у таблиці, на вихід передається код першого символу. Коли на вході читається черговий символ, для нього по таблиці перебуває рядок, що вже зустрічався, максимальної довжини, після чого в таблиці зберігається код цього рядка з наступним символом на вході; на вихід видається код цього рядка, а наступний символ використовується як початок наступного рядка.

Алгоритму декодування на вході потрібно тільки закодований текст, оскільки він може відтворити відповідну таблицю перетворення безпосередньо по закодованому тексту.

Алгоритм:

1. Ініціалізація словника всіма можливими односимвольними фразами. Ініціалізація вхідної фрази W першим символом повідомлення.
2. Знайти в словнику рядок W найбільшої довжини, яка збігається з останніми прийнятими символами.
3. Уважати черговий символ K з кодируемого повідомлення.
4. Якщо КІНЕЦЬ_ПОВІДОМЛЕННЯ, то видати код для W, інакше
5. Якщо фраза WK уже є в словнику, привласнити вхідній фразі W значення WK і перейти до Кроку 3, інакше видати код W, додати WK у словник, привласнити вхідній фразі W значення K і перейти до Кроку 3.
6. Кінець.

Наприклад, маємо алфавіт, закодований п'ятизначним кодом, причому три останні кодові комбінації залишаються невикористаними. Допустимо необхідно закодувати текст:

ПРОГАММААБРАКАТАБРАПРОБРАКИИБАРАКИ#

(34 літери, тобто необхідно 34х5=170 біт для їхньої передачі, # – знак закінчення тексту).

Процес кодування наведений у таблиці 1.12.

1	А	0 0 0 0 0	33	1 0 0 0 0 0
2	Б	0 0 0 0 1	34	1 0 0 0 0 1
3	В	0 0 0 1 0	35	1 0 0 0 1 0
4	Г	0 0 0 1 1	36	1 0 0 0 1 1
5	Д	0 0 1 0 0	37	1 0 0 1 0 0
6	Е	0 0 1 0 1	38	1 0 0 1 0 1
7	Є	0 0 1 1 0	39	1 0 0 1 1 0
8	Ж	0 0 1 1 1	40	1 0 0 1 1 1
9	З	0 1 0 0 0	41	1 0 1 0 0 0
10	І	0 1 0 0 1	42	1 0 1 0 0 1
11	И	0 1 0 1 0	43	1 0 1 0 1 0
12	К	0 1 0 1 1	44	1 0 1 0 1 1
13	Л	0 1 1 0 0	45	1 0 1 1 0 0
14	М	0 1 1 0 1	46	1 0 1 1 0 1
15	Н	0 1 1 1 0	47	1 0 1 1 1 0
16	О	0 1 1 1 1	48	1 0 1 1 1 1
17	П	1 0 0 0 0	49	1 1 0 0 0 0
18	Р	1 0 0 0 1	50	1 1 0 0 0 1
19	С	1 0 0 1 0	51	1 1 0 0 1 0
20	Т	1 0 0 1 1	52	1 1 0 0 1 1
21	У	1 0 1 0 0	53	1 1 0 1 0 0
22	Ф	1 0 1 0 1	54	1 1 0 1 0 1
23	Х	1 0 1 1 0	55	1 1 0 1 1 0
24	Ц	1 0 1 1 1	56	1 1 0 1 1 1
25	Ч	1 1 0 0 0	57	1 1 1 0 0 0
26	Ш	1 1 0 0 1	58	1 1 1 0 0 1
27	Щ	1 1 0 1 0	59	1 1 1 0 1 0
28	Ю	1 1 0 1 1	60	1 1 1 0 1 1
29	Я	1 1 1 0 0	61	1 1 1 1 0 0
30		1 1 1 0 1	62	1 1 1 1 0 1
31		1 1 1 1 0	63	1 1 1 1 1 0
32		1 1 1 1 1	64	1 1 1 1 1 1

Таблиця 1.12

Символ	Пошук у табл.	Код у канал	Новий запис у таблицю			Примітка
			Номер	Символ	Код	
П	П					
Р	Р, ПР	1 0 0 0 0 (П)	30	ПР	1 1 1 0 1	
О	О, РО	1 0 0 0 1 (Р)	31	РО	1 1 1 1 0	
Г	Г, ОГ	0 1 1 1 1 (О)	32	ОГ	1 1 1 1 1	5 бітні комбінації закінчені, далі використовуємо 6 бітні
А	А, ГА	0 0 0 1 1 (Г)	33	ГА	1 0 0 0 0 0	
М	М, АМ	0 0 0 0 0 (А)	34	АМ	1 0 0 0 0 1	
М	М, ММ	0 1 1 0 1 (М)	35	ММ	1 0 0 0 1 0	
А	А, МА	0 1 1 0 1 (М)	36	МА	1 0 0 0 1 1	
А	А, АА	0 0 0 0 0 (А)	37	АА	1 0 0 1 0 0	
Б	Б, АБ	0 0 0 0 0 (А)	38	АБ	1 0 0 1 0 1	
Р	Р, БР	0 0 0 0 1 (Б)	39	БР	1 0 0 1 1 0	
А	А, РА	1 0 0 0 1 (Р)	40	РА	1 0 0 1 1 1	
К	К, АК	0 0 0 0 0 (А)	41	АК	1 0 1 0 0 0	
А	А, КА	0 1 0 1 1 (К)	42	КА	1 0 1 0 0 1	
Т	Т, АТ	0 0 0 0 0 (А)	43	АТ	1 0 1 0 1 0	
А	А, ТА	1 0 0 1 1 (Т)	44	ТА	1 0 1 0 1 1	
Б	Б, АБ	–	–	–	–	АБ № 38
Р	Р, АБР	1 0 0 1 0 1 (АБ)	45	АБР	1 0 1 1 0 0	
А	А, РА	–	–	–	–	РА № 40
П	П, РАП	1 0 0 1 1 1 (РА)	46	РАП	1 0 1 1 0 1	

Продовження таблиці 1.12

Р	Р, ПР	–	–	–	–	ПР № 30
О	О, ПРО	1 1 1 0 1 (ПР)	47	ПРО	1 0 1 1 1 0	
Б	Б, ОБ	0 1 1 1 1 (О)	48	ОБ	1 0 1 1 1 1	
Р	Р, БР	–	–	–	–	БР № 39
А	А, БРА	1 0 0 1 1 0 (БР)	49	БРА	1 1 0 0 0 0	
К	К, АК	–	–	–	–	АК № 41
И	И, АКИ	1 0 1 0 0 0 (АК)	50	АКИ	1 1 0 0 0 1	
И	И, ИИ	0 1 0 1 0 (И)	51	ИИ	1 1 0 0 1 0	
Б	Б, ИБ	0 1 0 1 0 (И)	52	ИБ	1 1 0 0 1 1	
А	А, БА	0 0 0 0 1 (Б)	53	БА	1 1 0 1 0 0	
Р	Р, АР	0 0 0 0 0 (А)	54	АР	1 1 0 1 0 1	
А	А, РА	–	–	–	–	РА № 40
К	К, РАК	1 0 0 1 1 1 (РА)	55	РАК	1 1 0 1 1 0	
И	И, КИ	0 1 0 1 1 (К)	56	КИ	1 1 0 1 1 1	
#		0 1 0 1 0 (И)				

∑=23х5+5х6=145 (зменшення на 15%).

ТЕМА 2
ЗАВАДОСТІЙКЕ КОДУВАННЯ В СИСТЕМАХ ПЕРЕДАЧІ ДАНИХ

ЛЕКЦІЯ 1
ОСНОВИ ЗАВАДОСТІЙКОГО КОДУВАННЯ

1.1. Принцип побудови завадостійких кодів

Завадостійкими (коригувальними) кодами називаються коди, що дозволяють виявити або виправити в дискретних повідомленнях помилки, що виникають при передачі повідомлень по каналах зв'язку з перешкодами.

Застосування завадостійких кодів, як правило, пов'язане з розбивкою повідомлень на блоки з k елементів, називані k-елементними комбінаціями. У загальному випадку кожний елемент може приймати одне з q різних значень, тому такий код називається q-ковим. Параметр q називається основою коду.

У цей час найбільше поширення в передачі даних одержали коди з основою q=2.

Нехай z_i – довільна n-елементна двійкова комбінація, загальна кількість різних комбінацій довжини n рівно 2^n. Якщо з множини $Z=\{z_i\}$, $i = \overline{1, 2^n}$ вибрати за деяким правилом $N_k < 2^n$ комбінацій, то отримана множина $V=\{v_i\}$, $i = \overline{1, N_k}$, $\mathbf{V \in Z}$ буде **завадостійким кодом**. Комбінації v_i називаються кодовими або дозволеними комбінаціями, а комбінації $z_i \notin V$, які не входять у множину V – **забороненими комбінаціями**.

Застосування завадостійких кодів складається з двох етапів:

- кодування послідовності на передачі;
- декодування на прийомі.

Задача кодування – це завдання одержання при передачі для кожного k-елементного блоку відповідної йому ***n***-елементної комбінації з безлічі ***V.*** При цьому однозначна відповідність між блоками й кодовими комбінаціями можливо, якщо число блоків не перевищує N_k.

Завдання декодування – це завдання одержання *k*-елементного блоку із прийнятих ***n***-елементних комбінацій при одночасному виявленні або виправленні помилок.

При декодуванні завадостійкий код може використовуватися в трьох режимах:

- виявлення помилок;
- виправлення помилок;
- одночасне виправлення й виявлення помилок.

Виявлення помилок ілюструється на рисунку 2.1.

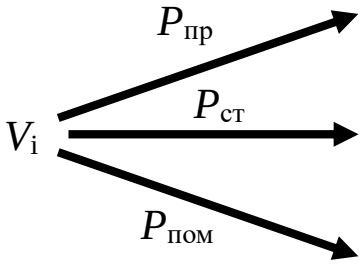


Рисунок 2.1 – Виправлення помилок

де $v_i \in V$ – правильне приймання; $z_i \in V$ – стирання (виявлена помилка); $v_j \in V$ – помилкове приймання (невиявлена помилка).

При передачі по каналу зв'язку деякої дозволеної комбінації на прийомній стороні можливі три несумісні результати:

– правильне приймання, що відповідає відсутності помилок у дискретному каналі зв'язку (імовірність події $P_{пр}$);

– приймання з виявленою помилкою, коли кодова комбінація під впливом помилок трансформується в заборонену (імовірність результату $P_{ст}$), при цьому формується сигнал стирання;

– приймання з невиявленою помилкою (імовірність події $P_{ош}$), що відповідає переходу під впливом помилок однієї дозволеної комбінації в іншу.

Оскільки три результати становлять повну групу подій, то справедлива рівність:

$$\boldsymbol{P_{пр}+P_{ст}+P_{ош}=1}$$

Виправлення помилок ілюструється на рисунку 2.2.

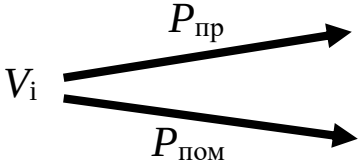


Рисунок 2.2 – Виправлення помилок

де $v_i \in v_i$ – правильне приймання; $z_i \in v_i$ – помилкове приймання.

При виправленні помилок множина Z розбивається на підмножини, у кожній підмножині V_i є одна дозволена комбінація v_i і деяка кількість заборонених комбінацій, якщо прийнята будь-яка комбінація, що входить у цю підмножину, то вважається, що передавалася дозволена комбінація v_i з нього. Підмножина V_i називається захисною зоною комбінації.

При передачі по каналу зв'язку деякої дозволеної комбінації v_i можливі наступні результати:

– правильне приймання, що відповідає влученню комбінації v_i у захисну зону V_i (імовірність події $P_{пр}$);

– помилкове приймання, коли перекручена під впливом помилок комбінація не попадає в захисну зону V_i і, отже, ідентифікується як інша дозволена комбінація (імовірність події $P_{ош}$). Очевидно, що

$$P_{пр} + P_{ош} = 1.$$

Приклад. Нехай n = 3, безліч дозволених комбінацій включає дві комбінації: $V_1 = 000, V_2 = 111$.

У випадку виявлення помилок усі інші комбінації крім 000 і 111 будуть забороненими й будуть стиратися.

У випадку виправлення при прийманні будь-якої комбінації з нулів або з однієї одиницею вважаємо що передавалася комбінація 000, усі 1 або не менш 2-х одиниць – передавалася комбінація 111.

Очевидний висновок з прикладу, що для реалізації можливості виявлення та виправлення помилок потрібно внести в кодові комбінації якусь надмірність.

Практична реалізація принципів завадостійкого кодування повинна забезпечити побудову безлічі дозволених комбінацій таким чином, щоб:

– максимізувати $P_{пр}$;

– мінімізувати складність кодеків.

1.2. Класифікація та параметри завадостійких кодів

У теорії й техніці завадостійкого кодування відома множина коректувальних кодів, які можуть бути класифіковані за різними ознаками. Класифікація кодів наведена на рисунку 2.3.

За способом формування КК підрозділяються на *блокові* й *неперервні*.

Формування *блокових* кодів передбачає розбивку переданих цифрових послідовностей на окремі блоки, які подаються на вхід кодера. Кожному такому блоку на виході кодера відповідає блок кодових символів, робота кодера визначається правилом, або алгоритмом кодування.

Формування *неперервних* кодів здійснюється неперервно в часі, без поділу на блоки, що й визначає найменування цього класу кодів. Блокові коди історично були запропоновані й вивчені раніше, на зорі розвитку теорії кодування.

У класі неперервних кодів слід зазначити *згорткові* коди, які за характеристиками перевершують блокові коди, і, з цієї причини, знаходять широке застосування в телекомунікаційних системах. Багато кодів носять імена вчених, які їх запропонували й досліджували. Таким прикладом є неперервний код Фінка-Хагельбаргера, запропонований радянським ученим Л.М. Фінком і німецьким фахівцем Р. Хагельбаргером. Тривалий час цей код

служив у літературі показовим прикладом неперервного коду із простим алгоритмом кодування/декодування, але після відкриття згорткових кодів поступився їм місце.

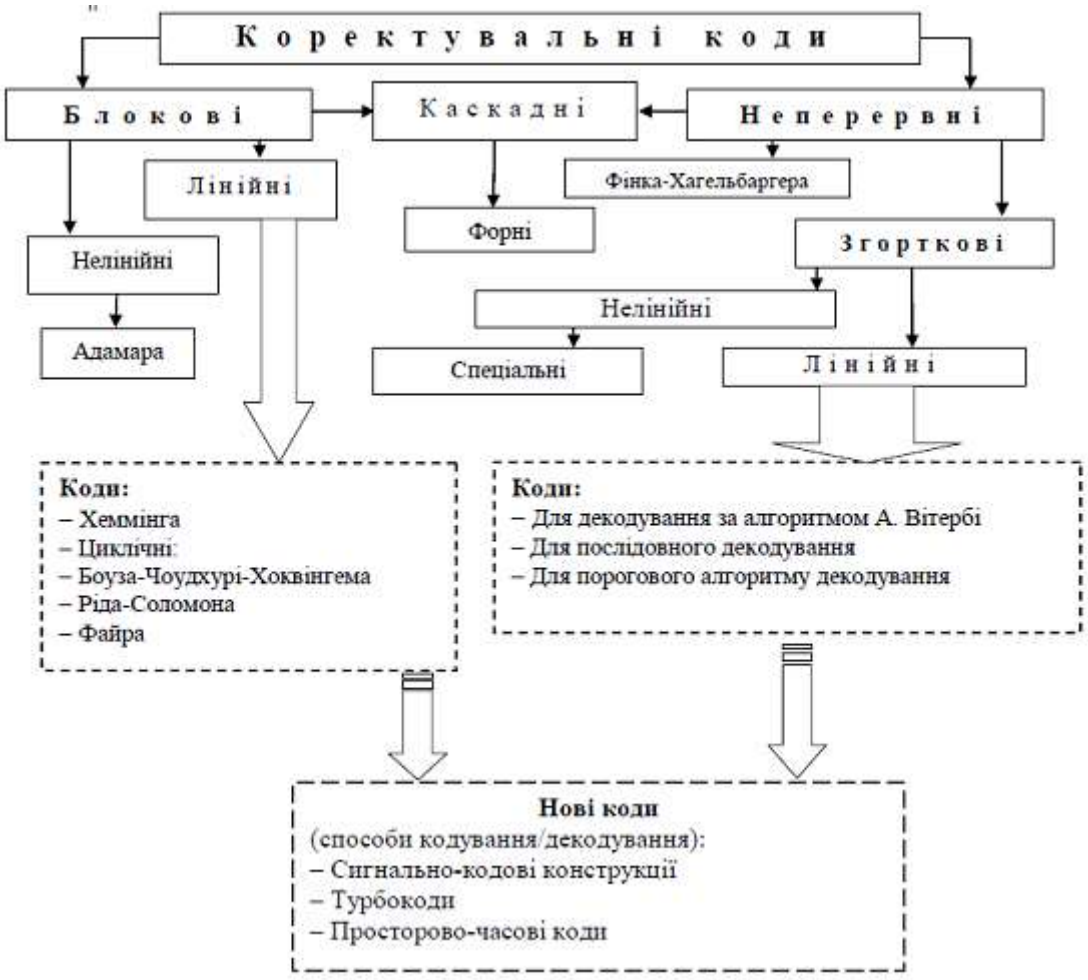


Рисунок 2.3 – Класифікація кодів

Для опису процедур кодування/декодування як блокових, так і згорткових кодів використовують адекватний математичний апарат. Для опису **лінійних** кодів використовується добре розроблений апарат лінійної алгебри. Формування **нелінійних** кодів виконується із застосуванням нелінійних процедур. Такий підхід дозволяє в деяких випадках одержати нелінійні коди з рядом спеціальних властивостей.

Відмітні переваги коректувальних кодів (як блокових, так і згорткових) спонукували пошуки нових підходів до реалізації шляхів підвищення завадостійкості й ефективності телекомунікаційних систем. На рис. 3 відзначені, відповідно, нові методи кодування: сигнально-кодові конструкції, турбокоди, просторово-часові коди й т.п, які утворені в результаті симбіозу блокових та неперервних кодів.

Інколи вводять також поняття **систематичних** (роздільних) та **несистематичних** (нероздільних) кодів, які відрізняються можливістю відокремлення інформаційної послідовності від перевірних символів у

закодованому сигналі. така класифікація справедлива як для блокових так і для неперервних кодів.

Основні параметри завадостійких кодів

Комбінація $A=(a_0a_1... a_{n-1})$, де a_i – елементи, значення яких рівні 0 або 1, характеризується вагою:

$$W \sum_i a_i,$$

тобто числом одиниць у ній.

Нехай $A=(a_0a_1... a_{n-1})$ і $B=(b_0b_1... b_{n-1})$ n-елементні комбінації. Відстань Хемінга між A и B – d_{ab} дорівнює ваги суми цих комбінацій по модулю 2 або кількості незбіжних елементів з однаковими індексами і у цих комбінаціях.

Для оцінки властивостей завадостійкого коду використовують наступні основні параметри:

– *довжина* кодової комбінації n;

– *число дозволених* комбінацій $N_k=2^k$;

– *кількість всіх* комбінацій $N=2^n$;

– *абсолютна надмірність* $r = n - \log_2 N_k$. Для роздільних кодів ***r= n–k;***

– *відносна надмірність* або *швидкість* передачі коду R= k/n. ***R – характеризує ефективність використання каналу зв'язку;***

– *коефіцієнт надмірності* систематичних кодів К=1 – $R = (n – k)/n$.

У **систематичних** кодах кожна кодова комбінація довжиною n символів містить k інформаційних символів. При цьому r = n–k додаткових символів, які залежать від інформаційних символів, використовуються при декодуванні для виявлення або виправлення помилок.

У **несистематичних** кодах інформаційні символи в явному виді в кодовій комбінації не містяться.

Мінімальна кодова відстань d_{min} – найменше з попарних відстаней Хемінга в множині дозволених комбінацій завадостійкого коду.

d_{min} однозначно визначає максимально гарантовану кратність, що виявляються S, що й виправляються t помилок. **Для режиму виявлення помилок** $S = d_{min}–1 \rightarrow d_{min}= S+1$, тобто мінімальна кодова відстань повинна бути на 1 більше чому припустима кількість помилок, що виявляються. Інакше зміна в комбінації внаслідок помилок більшого числа елементів може привести до переходу однієї дозволеної комбінації в іншу.

Для режиму виправлення помилок:

– $t = (d_{min}–1)/2$ або $d_{min}= 2t+1$ для непарних d_{min};

– $t = (d_{min}–2)/2$ або $d_{min}= 2t+2$ для парних d_{min}.

Наприклад, якщо d_{min} = 5 ((5–1)/2=2), те одно- і двократні помилки виправляються. Помилки кратності більш, ніж два, визначаються, як з помилками.

При одночасному виправленні й виявленні помилок d_{min}, S і t зв'язані співвідношенням d_{min} = t+ S+1, S≥ t, яке є узагальнюючим для розглянутих вище випадків.

Наприклад, d_{min} = 5 можливі наступні режими використання коду:

– виявлення помилок кратності 4 і менш (t = 0, S =4);

– виправлення одно- і двократних помилок (t = S =2);

– одночасне виправлення однократних (t=1) і виявлення помилок кратності ≤3 (S = 3).

1.3. Декодування завадостійких кодів

Граничні співвідношення між параметрами завадостійких кодів

Одним з найважливіших завдань побудови завадостійкого коду із заданими характеристиками є встановлення співвідношення між його здатністю виявляти або виправляти помилки й надмірністю.

Розглянемо граничні оцінки, що зв'язують d_{min}, n і k.

Нехай код призначений для виправлення помилок кратності t, тоді існує граничне співвідношення Хемінга:

$$n - k \geq \log_2 \sum_{i=0}^{t} C_n^i,$$

де $C_n^i = \frac{n!}{i!(n-i)!}$.

Це співвідношення задає мінімальну надмірність при якій можливе виявляти або виправляти помилки.

Розглянемо основні принципи декодування блокових і безперервних кодів, які використовують у режимі виправлення або одночасного виправлення й виявлення помилок.

Найпоширенішим способом виправлення помилок блоковим кодом є декодування по максимуму правдоподібності.

Спосіб декодування по методу максимальної правдоподібності заснований на наступному очевидному положенні: імовірність викривлення кодової комбінації зменшується з ростом кратності помилок, тобто *P(i,n) > P (i+1,n).* Тому представляється природнім ототожнювати прийняту комбінацію з кодовою комбінацією, що відстоїть від неї на найменшу відстань.

Процедура виправлення помилок реалізується в наступній послідовності:

– Обчислюється відстань Хемінга d між прийнятою комбінацією z і всіма дозволеними комбінаціями $\{v_i\}$, $i = \overline{1, 2^k}$.

– Прийнята комбінація z ототожнюється з кодовою комбінацією для якої справедливо $d = \min d_i$.

Слід зазначити, що розв'язок може бути не єдиним, тому необхідно передбачити додаткову процедуру вибору з декількох можливих кодових комбінацій єдиної.

При використанні безперервних кодів виправлення помилок здійснюється такими способами:

– спосіб граничного декодування;
– спосіб послідовного декодування;
– спосіб декодування по максимуму правдоподібності.

Через те, що довжина комбінацій безперервного коду досить велика (у загальному випадку, квазінескінченна), то прийняття рішення про наявність і виправлення помилок проводиться на основі аналізу відрізків (сегментів) комбінацій кінцевої довжини з урахуванням взаємозалежності цих сегментів.

Граничне декодування полягає в тому, що при прийманні комбінацій безперервного коду формується перевірочний вектор спеціального виду й аналізується його структура. У результаті визначаються й інвертуються елементи комбінації, викривлення яких приводить до ідентичної або схожій структурі вектора перевірок. Аналіз комбінацій і ідентифікація перекручених елементів здійснюється за допомогою граничних схем, що працюють по мажоритарному принципу.

Спосіб граничного декодування заснований на простих ідеях і знаходить досить широке застосування на практиці. Алгоритми декодування, як правило, розробляються для конкретних типів кодів, принципи побудови яких допускають ефективну реалізацію цих алгоритмів.

Послідовне декодування засноване на інтерпретації процесу формування кодових комбінацій як процедури побудови деякого дерева, при цьому кожному шляху відповідає дозволена комбінація. При декодуванні прийнятої комбінації по кодовому дереву послідовно визначається шлях, а, отже, деяка кодова комбінація v_i така, що умовна ймовірність $P(v_i/z)$ максимальна. Особливістю практичної реалізації способу є необхідність наявності в декодері запам'ятовувального пристрою досить великої ємності для зберігання прийнятих послідовностей і результатів пошуку найбільш імовірного шляху, причому, чим нижче якість дискретного каналу зв'язку, тем більший обсяг пам'яті буде використовуватися.

Найпоширенішими процедурами послідовного декодування є алгоритм Фано й стік-алгоритм.

Виправлення помилок по максимуму правдоподібності проводиться за аналогією з декодуванням блокових кодів, відмінність полягає в тому, що

рішення ухвалюються на послідовності взаємозалежних відрізків прийнятої послідовності.

До цього методу відносять алгоритм Вітербі, який вважається найбільш ефективним алгоритмом декодування, що здійснює ітеративну обробку послідовності сегментів і базований на методах динамічного програмування.

ТЕМА 3
ПРИНЦИПИ РЕАЛІЗАЦІЇ ФУНКЦІЙ ОБЛАДНАННЯ МЕРЕЖ ПЕРЕДАЧІ ДАНИХ

ЛЕКЦІЯ 1
ОПЕРАЦІЙНА СИСТЕМА CISCO IOS

1.1. Компоненти пам’яті та порядок завантаження

В основі більшості технологій корпорації Cisco лежить спеціалізована операційна система – **міжмережева операційна система корпорації Cisco (Internetwork Operating System – IOS)**, яка являє собою специфічне програмне забезпечення для керування функціями маршрутизації та комутації.

Маршрутизатор має доступ до енергозалежної або незалежній пам'яті. Енергозалежною пам'яті для збереження даних потрібне постійне живлення. При виключенні електроживлення маршрутизатора або при його перезапуску вміст цієї пам'яті втрачається. Незалежна пам'ять зберігає дані навіть при перезавантаженні пристрою. У зв'язку з цим в маршрутизаторі Cisco використовується чотири типи пам'яті (рисунок 3.1):

Оперативний запам’ятовуючий пристрій (ОЗП) (RAM). Це незалежна пам'ять використовується в маршрутизаторах Cisco для зберігання додатків, процесів і даних, необхідних для їх обробки центральним процесором. Маршрутизатор Cisco використовують швидкий тип ОЗП, званий синхронним динамічним ОЗП (SDRAM). Натисніть зображення ОЗП на малюнку, щоб подивитися додаткову інформацію.

Постійний запам’ятовуючий пристрій (ПЗП) (ROM). Ця незалежна пам'ять використовується для зберігання важливих інструкцій по експлуатації та обмеженої версії IOS. Таким чином, ПЗП – це вбудована в мікросхему мікропрограма всередині маршрутизатора, яка може бути змінена тільки компанією Cisco. Натисніть зображення ПЗП на малюнку, щоб подивитися додаткову інформацію.

NVRAM. Ця незалежна пам'ять використовується як місце постійного зберігання файлу завантажувального конфігурації (startup-config).

Флеш. Це незалежна пам'ять комп'ютера, що використовується в якості місця постійного зберігання IOS і інших системних файлів, таких як файли журналів, файли голосового конфігурації, HTML файли, конфігурації резервного копіювання та багато іншого. При перезавантаженні маршрутизатора IOS копіюється з флеш-пам'яті в ОЗП.

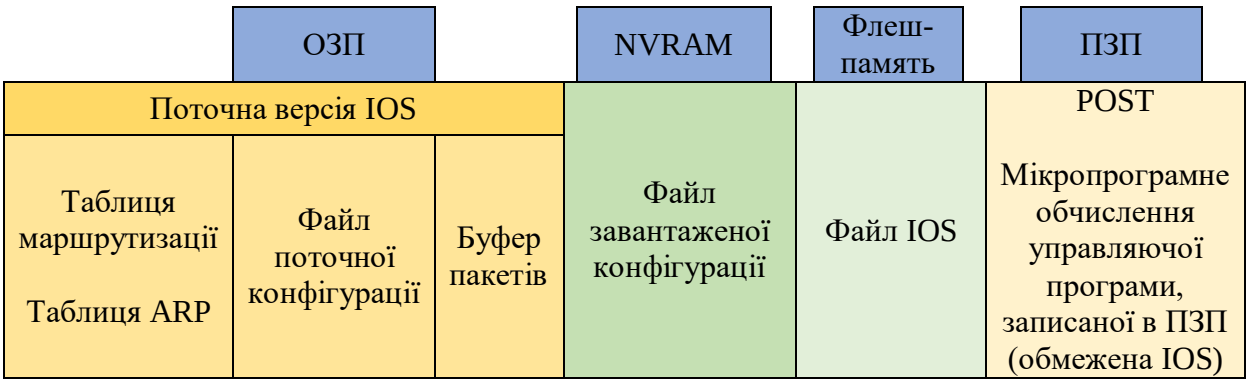


Рисунок 3.1 – Типи пам’яті

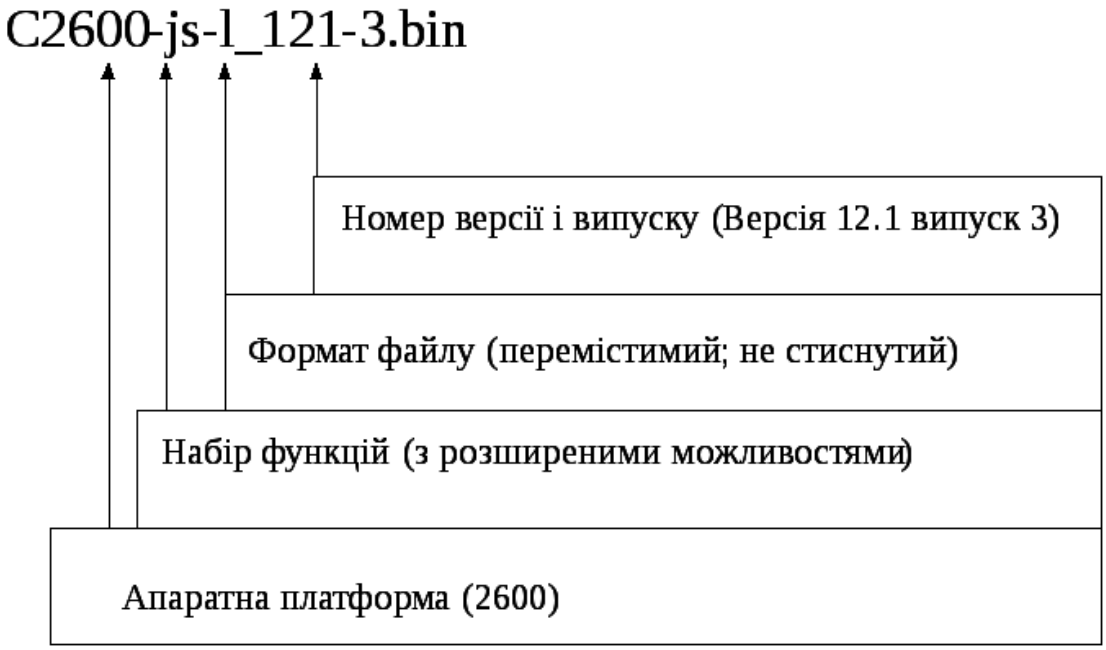


Рисунок 3.2 – Прийняті корпорацією Cisco позначення імені файлу

Як показано на рисунку 3.2, погодження про позначення описують **значення декількох полів в імені файлу:**

– **Апаратна платформа.** Перша частина імені файлу вказує апаратну платформу, для якої призначена ця версія.

– **Набір функцій**. Друга частина імені файлу характеризує різні функції, які реалізує цей файл. Користувач може вибрати будь-які набори функцій, які упаковані в образи програмного забезпечення. Кожен набір функцій містить певну підмножину з усього набору функцій програмного забезпечення CiscoIOS. Приклади таких наборів наведено нижче.

– **Базовий набір (Basic)**. Включає в себе основні функції для всіх апаратних платформ. Прикладом функцій базового набору є підтримка протоколів IPiIP/FW.

– **Додаткові функції (набір Plus)**. Набір Plus являє собою базовий набір, до якого додані такі додаткові функції, як Plus, IP/FW Plus і Enterprise Plus.

– **Шифрування.** Цей набір містить функції 56-бітового шифрування даних, додані до набору Basic або набору Plus. Прикладами набору

шифрування можуть служити IP/ATM PLUS IPSEC 56 і Enterprise Plus 56. Починаючи з версії 12.2, у версіях Cisco IOS для позначення шифрування використовуються ідентифікатори k8/k9. У версії 12.2 і пізніших ідентифікатор k8 вказує на 64-бітове шифрування або шифрування з меншою кількістю бітів, в той час як k9 вказує на 64-бітове шифрування або шифрування з великою кількістю бітів.

– **Формат файлу**. Третя частина імені файлу IOS вказує його формат. Вона показує, чи зберігається програмне забезпечення IOS Cisco в Flash-пам'яті в стислому вигляді (форматі) і чи допускає образ IOS Cisco переміщення. Якщо Flash-образ зберігається в стислому вигляді, то в процесі завантаження він повинен бути розпакований, а сам образ скопійований в оперативну пам'ять RAM. Якщо образ допускає переміщення, він може бути скопійований в пам'ять RAM і запущений з неї. Непереміщуємий образ запускається безпосередньо з Flash-пам'яті.

– **Версія і випуск**. У четвертій частині імені файлу вказується номер версії і випуску. У міру того, як розробляються нові версії IOS Cisco, номер версії зростає.

Твердження про іменування образів операційної системи Cisco IOS, функції певних образів операційної системи та багато іншого може бути в майбутньому змінено.

При виборі нової версії операційної системи Cisco IOS перш за все слід розглянути вимоги до обсягу оперативної і Flash-пам'яті. Зазвичай, чим новішаверсія операційної системи, тим більше функцій в неї включено, отже, тим більших апаратних ресурсів, зокрема, пам'яті вони будуть вимагати.

Для перевірки поточної версії операційної системи та вільної Flash-пам'яті використовуйте команду ***show version***.

Всі платформи маршрутизатора мають параметри і компоненти за замовчуванням. Наприклад, маршрутизатори Cisco 1941 поставляються разом з пам'яттю SDRAM об'ємом 512 МБ, яка може бути розширена до 2,0 ГБ. Маршрутизатор Cisco тисяча дев'ятсот сорок одна також поставляються разом з флеш-пам'яттю об'ємом 256 МБ, яка може бути розширена за допомогою двох зовнішніх слотів Compact Flash. Кожен слот підтримує високошвидкісні карти пам'яті ємністю до 4 ГБ. Клацніть тут, щоб дізнатися додаткову інформацію про маршрутизатор з інтегрованими сервісами Cisco 1941.

Після включення мережеве обладнання Cisco проходить наступні стадії завантаження:

– По-перше, пристрій завантажує програму самотестування при включенні живлення (POST), що зберігається в ПЗУ. POST перевіряє ЦБ підсистеми. Програма тестує ЦБ, оперативну динамічну пам'ять (DRAM) і частину флеш-пристроїв, яка складає файлову систему флеш-пам'яті.

– Після цього на пристрої запускається програмне забезпечення початкового завантажувача. Початковий завантажувач – це невелика програма, яка зберігається в ПЗУ і запускається відразу після успішного завершення перевірки POST. Початковий завантажувач виконує низькрівневу

ініціалізацію ЦП. Він ініціалізує регістри ЦП, які контролюють фізичну пам'ять, обсяг пам'яті і швидкість.

– Потім програма запускає файлову систему флеш-пам'яті на материнській платі.

– Нарешті, початковий завантажувач знаходить і завантажує образ операційної системи IOS за замовчуванням і передає їй управління пристроєм.

– Операційна система IOS знаходить файл конфігурації і завантажує його.

1.2. Протокол TFTP

Для збереження та відновлення конфігураційних файлів, а при необхідності – образів операційної системи, використовується протокол TFTP (Trivial File Transfer Protocol – спрощений протокол передачі файлів). Він є дуже простим і підтримується будь-яким обладнанням, в тому числі програмою початкового завантаження обладнання Cisco. Обмін відбувається з мережним вузлом, на якому встановлено програмне забезпечення TFTP-сервера.

Обмін між клієнтом і сервером починається з того, що клієнт запитує сервер або прочитати, або записати файл для клієнта. У стандартному варіанті завантаження бездисковой системи перший запит – це запит на читання (RRQ). На рисунку 3.3 показаний формат п'яти повідомлень TFTP. (Коди операцій 1 і 2 мають однаковий формат.)

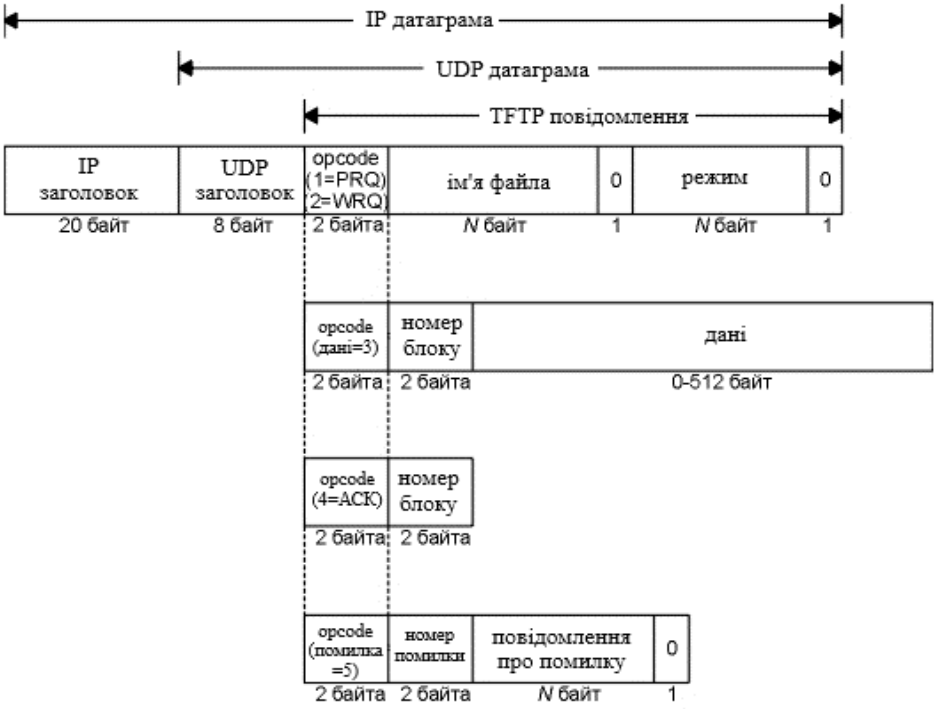


Рисунок 3.3 – Формат п’яти TFTP повідомлень

де opcode – код операції.

У TFTP існує 2 режиму передачі:

– **netascii** – файл перед передачею перекодируется в ASCII.
– **octet** – файл передається без змін.

Кожен пакет даних містить номер блоку (block number), який потім використовується в пакеті підтвердження. Як приклад скажімо, що коли необхідно здійснити читання файлу, клієнт посилає запит на читання (RRQ), вказуючи ім'я файлу і режим. Якщо файл може бути прочитаний клієнтом, сервер відповідає пакетом даних з номером блоку рівним 1. Клієнт посилає підтвердження (ACK) на номер блоку 1. Сервер відповідає наступним пакетом даних з номером блоку рівним 2. Клієнт підтверджує номер блоку 2. Це триває доти , поки файл не буде переданий. Кожен пакет даних містить 512 байт даних, за винятком останнього пакета, який містить від 0 до 511 байт даних. Коли клієнт отримує пакет даних, який містить менше ніж 512 байт, він вважає, що отримав останній пакет.

У разі запиту на запис (WRQ) клієнт посилає WRQ, вказуючи ім'я файлу і режим. Якщо файл може бути записаний клієнтом, сервер відповідає підтвердженням (ACK) з номером блоку рівним 0. Клієнт посилає перші 512 байт файлу з номером блоку рівним 1, сервер відповідає ACK з номером блоку рівним 1.

Цей тип передачі даних називається протоколом із зупинкою і очікуванням підтвердження (stop-and-wait). Він використовується тільки в простих протоколах, таких як TFTP.

Останній тип TFTP повідомлень це повідомлення про помилки, код операції (opcode) дорівнює 5. Це якраз те, чим сервер відповідає в тому випадку, якщо запит на читання або запис не може бути оброблений. Помилки читання або запису в перебігу передачі файлу також призводять до того, що відправляється повідомлення про помилку, при цьому передача припиняється. Номер помилки (error number) містить цифровий код помилки, за яким слід повідомлення про помилку в ASCII форматі, яке може містити додаткову інформацію надану операційною системою.

Так як TFTP використовує ненадійний UDP, то саме від TFTP залежить, як будуть опрацьовані втрачені і дубльовані пакети. У разі втрати пакету, відправник відпрацьовує тайм-аут і здійснює повторну передачу.

TFTP пакети (рис. 3) не містять ніяких даних про ім'я користувача або пароль. Це пролом в секретності характерна для TFTP. Так як TFTP був розроблений для використання в процесі завантаження, він не надає можливості передати ім'я користувача і пароль.

Ця характеристика TFTP була використана багатьма хакерами, щоб отримати копії файлу паролів з Unix і потім розшифрувати паролі. Щоб запобігти подібному доступ, більшість TFTP серверів в даний час регламентують, які файли можуть бути отримані з використанням TFTP (як правило, файли з директорії / tftpboot в Unix системах). Ця директорія містить тільки завантажувальні файли, необхідні бездисковий системам.

TFTP – це простий протокол, розроблений таким чином, щоб поміщатися в ПЗУ і бути використаним тільки в процесі завантаження

бездискових систем. Він використовує невелику кількість форматів повідомлень і протокол із зупинкою і очікуванням підтвердження.

Щоб дозволити кільком клієнтам завантажуватися одночасно, TFTP сервер надає кілька форм одночасної роботи. Так як UDP не надає унікального з'єднання між клієнтом і сервером (як це робить TCP), TFTP сервер створює новий UDP порт для кожного клієнта. Це дозволяє різним клієнтам видавати датаграми, які будуть демультіплексіровать UDP модулем сервера, на основі номерів портів призначення, замість того щоб це робив сам сервер.

1.3. Збереження та відновлення конфігураційних файлів та операційної системи на TFTP-сервері

Файлова система Cisco IOS (IFS) дозволяє адміністратору переміщатися по різним каталогам і перераховувати файли в каталозі. Адміністратор також може створювати підкаталоги у флеш-пам'яті або на диску. Доступні каталоги залежать від пристрою.

Команда **show file systems** надає корисну інформацію (рисунку 3.4), таку як обсяг загальної і вільної пам'яті, тип файлової системи і її дозволу. Дозволи включають тільки читання (ro), тільки запис (wo) і читання і запис (rw). Права доступу відображаються в стовпці «Прапори» вихідних даних команди.

```
Router# show file systems
File Systems:
      Size(b)       Free(b)      Type  Flags  Prefixes
            -             -    opaque     rw  system:
            -             -    opaque     rw  tmpsys:
*  7194652672    6294822912      disk     rw  bootflash: flash:
    256589824     256573440      disk     rw  usb0:
   1804468224    1723789312      disk     ro  webui:
            -             -    opaque     rw  null:
            -             -    opaque     ro  tar:
            -             -   network     rw  tftp:
            -             -    opaque     wo  syslog:
     33554432      33539983      nvram     rw  nvram:
            -             -   network     rw  rcp:
            -             -   network     rw  ftp:
            -             -   network     rw  http:
            -             -   network     rw  scp:
            -             -   network     rw  sftp:
            -             -   network     rw  https:
            -             -    opaque     ro  cns:
Router#
```

Рисунок 3.4 – Використання команди **show file systems**

Хоча в списку кілька файлових систем, нас цікавлять файлові системи tftp, flash і nvram.

Зверніть увагу, що файлової системи флеш-пам'яті також передує зірочка. Це вказує на те, що flash є поточної файлової системою за замовчуванням. Завантажувальний IOS знаходиться у флеш-пам'яті; тому символ (bootflash) додається до списку флеш-пам'яті, вказуючи, що це завантажувальний диск.

Файлова система Flash відображається командою **dir (directory)**. Її вихідні дані на рисунку 3.5. Оскільки flash є файлової системою за замовчуванням, команда dir виводить вміст flash.

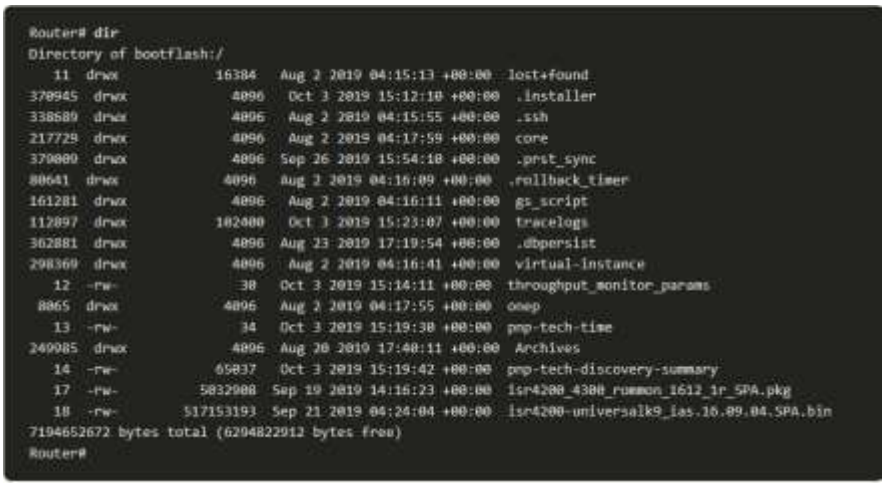


Рисунок 3.5 – Відображення файлової системи Flash за допомогою команди **dir**

Кілька файлів знаходяться у флеш-пам'яті, але особливий інтерес представляє останній зі списку. Це ім'я поточного способу файлу Cisco IOS, що працює в оперативній пам'яті.

Щоб переглянути вміст NVRAM, потрібно змінити поточну файлову систему за замовчуванням за допомогою команди **cd** (змінити каталог), як показано на рисунку 3.6.

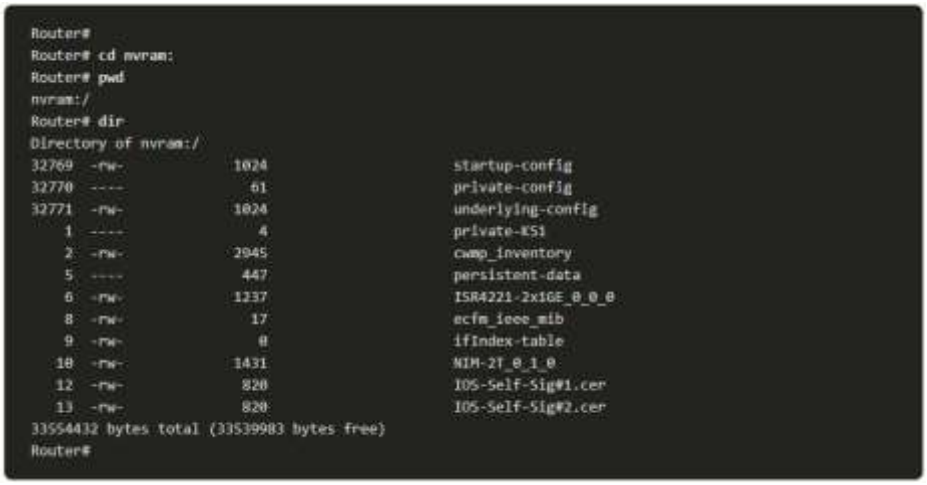


Рисунок 3.6 – Відображення вмісту NVRAM за допомогою команди **cd**

Команда робочого каталогу – **pwd** перевіряє, що йде перегляд каталогу NVRAM. Команда dir виводить вміст NVRAM. Хоча в списку кілька файлів конфігурації, особливий інтерес представляє файл конфігурації запуску (startup-config).

Конфігурацію можна скопіювати з файлу, а потім безпосередньо вставити на пристрій. IOS виконує кожен рядок тексту конфігурації у вигляді

команди. Це означає, що файл конфігурації потребуватиме попередньому редагуванні, щоб зашифровані паролі були в незашифрованому вигляді, а текст, який не є командою, такою як - More - і повідомлення IOS, був вилучений. Перед вставкою конфігурації необхідно увійти в режим глобальної конфігурації.

Використання TFTP для резервного копіювання конфігурації

Копії файлів конфігурації можуть зберігатися як резервні файли на випадок виникнення проблем. Файли конфігурації можуть зберігатися на сервері TFTP або на USB-накопичувачі. Файл конфігурації також повинен бути включений в мережеву документацію.

Щоб зберегти поточну конфігурацію або конфігурацію запуску на TFTP-сервері, використовують команду **copy running-config tftp** або **copy startup-config tftp**, як показано на рисунку 3.7.

Рисунок 3.7 – Використання команди **copy running-config tftp**

Дії для резервного копіювання працює конфігурації на TFTP-сервер:

Крок 1. Ввести команду **copy running-config tftp**.

Крок 2. Ввести IP-адреса хоста, на якому буде зберігатися файл конфігурації.

Крок 3. Ввести ім'я, яке потрібно присвоїти файлу конфігурації.

Крок 4. Натиснути Enter, щоб підтвердити кожен вибір.

Щоб відновити поточну або початкову конфігурацію з TFTP-сервера, використовують команду **copy tftp running-config** або **copy tftp startup-config**. Для відновлення конфігурації з TFTP-сервера необхідно:

Крок 1. Ввести команду **copy tftp running-config**.

Крок 2. Ввести IP-адреса хоста, на якому зберігається файл конфігурації.

Крок 3. Ввести ім'я, яке потрібно присвоїти файлу конфігурації.

Крок 4. Натиснути Enter, щоб підтвердити кожен вибір.

Деякі моделі маршрутизаторів Cisco підтримують USB-накопичувачі. Функція USB-флеш-пам'яті забезпечує додаткову можливість додаткового зберігання і додаткове завантажувальний пристрій. Зображення, конфігурації та інші файли можна копіювати на флеш-пам'ять Cisco USB або з неї з тієї ж надійністю, що і при зберіганні та отриманні файлів з використанням карти Compact Flash. Крім того, модульні інтегровані сервісні маршрутизатори можуть завантажувати будь-який образ програмного забезпечення Cisco IOS, збережений на флеш-пам'яті USB. В ідеалі USB-накопичувач може зберігати кілька копій Cisco IOS і кілька конфігурацій маршрутизатора.

Команду **dir** використовують для перегляду змісту флеш-накопичувача USB, як показано на рисунку 3.8.

```
Router# dir usbflash0:
Directory of usbflash0:/
1 -rw- 30125020 Dec 22 2032 05:31:32 +00:00 c3825-entservicesk9-mz.123-14.T
63158272 bytes total (33033216 bytes free)
```

Рисунок 3.8 – Використання команди **dir** для перегляду змісту флеш-накопичувача USB

Під час резервного копіювання на USB-порт рекомендується виконати команду **show file systems**, щоб переконатися в наявності USB-накопичувача і підтвердити його ім'я. В останньому рядку виведення відображається порт USB і ім'я: «usbflash0:».

Команда **copy run usbflash0: /** застосовується щоб скопіювати файл конфігурації на USB-накопичувач. Обов'язково використовують ім'я флешки, як зазначено в файлової системі. Коса риска є необов'язковою, але вказує на кореневої каталог флеш-накопичувача USB. IOS запросить ім'я файлу. Якщо файл вже існує на USB-накопичувачі, маршрутизатор запропонує перезаписати, можливо і копіювання на флеш-накопичувач USB без раніше створеного файлу, із запитом імені.

Команду **dir** використовують щоб переглянути файл на USB-накопичувачі, і команду more, щоб переглянути вміст, як показано на рисунку 3.9.

```
R1# dir usbflash0:/
Directory of usbflash0:/
    1  drw-     0  Oct 15 2010 16:28:30 +00:00  Cisco
   16  -rw-  5024  Jan 7 2013 20:26:50 +00:00  R1-Config
4050042880 bytes total (3774144512 bytes free)
R1#
R1# more usbflash0:/R1-Config
!
! Last configuration change at 20:19:54 UTC Mon Jan 7 2013 by
admin version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
```

Рисунок 3.9 – Використання команди **dir** для перегляду файлів на USB-накопичувачі

Щоб скопіювати файл назад, необхідно відредагувати файл USB R1-Config за допомогою текстового редактора. Припускаючи, що ім'я файлу - R1-Config, використовують команду copy usbflash0: / R1-Config running-config, щоб відновити робочу конфігурацію.

Процедури відновлення пароля

Паролі на пристроях використовуються для запобігання несанкціонованому доступу. Для зашифрованих паролів, таких як включення

секретних паролів, паролі повинні бути замінені після відновлення. Детальна процедура відновлення пароля залежить від пристрою. Однак всі процедури відновлення пароля засновані на тому ж принципі:

Крок 1. Увійти в режим ROMMON.

Крок 2. Змінити регістр конфігурації.

Крок 3. Скопіювати початковий конфігураційний файл в поточний.

Крок 4. Змінити пароль.

Крок 5. Зберегти running-config як новий startup-config.

Крок 6. Перезавантажити пристрій.

Для відновлення пароля потрібно консольний доступ до пристрою через програмне забезпечення терміналу або емулятора терміналу на ПК. Налаштування терміналу для доступу до пристрою: 9600 біт, без перевірки парності, 8 біт даних, 1 стоповий біт, немає управління потоком.

Крок 1. Увійдіть в режим ROMMON.

За допомогою доступу до консолі користувач може отримати доступ до режиму ROMMON, використовуючи комбінацію переривання під час процесу завантаження або витягуючи зовнішню флеш-пам'ять, коли пристрій вимкнений. У разі успіху з'явиться запрошення rommon 1>, як показано на рисунку 3.10.

Комбінація переривання для PuTTY: Ctrl + Break. Список стандартних комбінацій клавіш переривання для інших емуляторів терміналу і операційних систем можна знайти в Інтернеті.

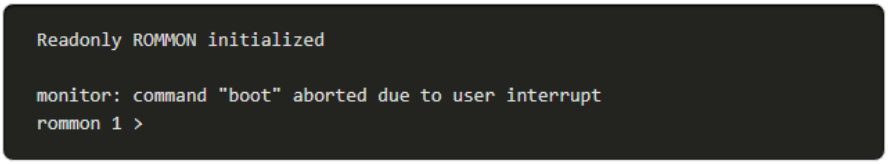


Рисунок 3.10 – Варіант доступу до режиму ROMMON

Крок 2. Зміна регістра конфігурації.

Програмне забезпечення ROMMON підтримує деякі основні команди, такі як **confreg**. Команда confreg 0x2142 дозволяє користувачеві встановити регістр конфігурації на 0x2142 (рисунок 3.11). З регістром конфігурації 0x2142 пристрій ігноруватиме файл конфігурації запуску при запуску. Файл конфігурації запуску, де знаходяться неіхвестние паролі. Щоб перезавантажити пристрій після установки регістра конфігурації в 0x2142, необхідно ввести в командному рядку **reset**.

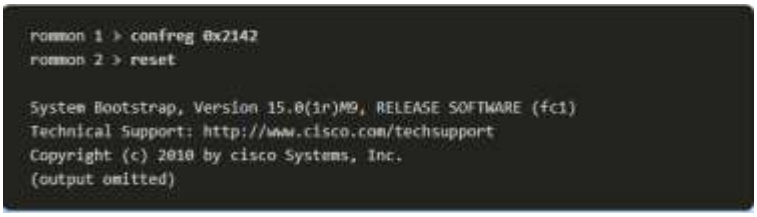


Рисунок 3.11 – Використання команди confreg 0x2142

Крок 3. Копіювання стартової конфігурації startup-config в поточну конфігурацію running-config.

Після завершення перезавантаження пристрою скопіюйте початкову конфігурацію в робочу конфігурацію за допомогою команди **copy startup-config running-config**, як показано в прикладі. Зверніть увагу, що запрошення маршрутизатора змінилося на R1 #, тому що ім'я хоста встановлено в R1 в startup-config (рисунок 3.12).

УВАГА: Не вводьте команду copy running-config startup-config. Ця команда стирає вихідну конфігурацію запуску.

```
Router# copy startup-config running-config
Destination filename [running-config]?

1450 bytes copied in 0.156 secs (9295 bytes/sec)
R1#
```

Рисунок 3.12 – Використання команди **copy startup-config running-config**

Крок 4. Зміна пароля.

Перебуваючи в привілейованому режимі EXEC, можна налаштувати всі необхідні паролі, як показано на рисунку 3.13.

```
R1# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)# enable secret cisco
```

Рисунок 3.13 – Варіант налаштування всіх необхідних паролей

Крок 5. Збереження running-config як нового startup-config.

Після настройки нових паролів треба змінити регістр конфігурації назад на 0x2102 за допомогою команди **config-register 0x2102** в режимі глобальної конфігурації і зберегти running-config в startup-config, як показано на рисунку 3.14.

```
R1(config)# config-register 0x2102
R1(config)# end
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

Рисунок 3.14 – Використання команди **config-register 0x2102**

Крок 6. Перезавантаження пристрою.

Тепер пристрій використовує знову налаштовані паролі для аутентифікації і його можна перезавантажити командою **reload**. Обов'язково використовуйте команди show, щоб переконатися, що всі зміни все ще на місці. Наприклад, переконайтеся, що відповідні інтерфейси не закриті після відновлення пароля.

TFTP-сервери як резервне сховище

У міру зростання мережі образи програмного забезпечення Cisco IOS і файли конфігурації можуть зберігатися на центральному сервері TFTP, як показано на рисунку 3.15. Це допомагає контролювати кількість образів IOS і версій цих образів IOS, а також файлів конфігурації, які необхідно підтримувати.

Рисунок 3.15 – Зберігання файлів конфігурації на центральному сервері TFTP

Корпоративні мережі зазвичай охоплюють широкі області і містять кілька маршрутизаторів. Для будь-якої мережі рекомендується зберігати резервну копію образу програмного забезпечення Cisco IOS на випадок, якщо образ системи на маршрутизаторі буде пошкоджений або випадково видалений.

Широко розподіленим маршрутизаторів потрібно джерело або резервна копія для образів програмного забезпечення Cisco IOS. Використання мережевого TFTP-сервера дозволяє завантажувати образ або його конфігурацію по мережі. Мережевим TFTP-сервером може бути інший маршрутизатор, робоча станція або хост-система.

Щоб підтримувати мережеві операції з мінімальним часом простою, необхідно мати процедури для резервного копіювання образів Cisco IOS. Це дозволяє адміністратора швидко скопіювати зображення назад на маршрутизатор в разі пошкодження або стирання образу.

На малюнку 16 адміністратор мережі хоче створити резервну копію поточного файлу образу маршрутизатора (isr4200-universalk9_ias.16.09.04.SPA.bin) на сервері TFTP за адресою 172.16.1.100.

Крок 1. Перевірка зв'язку з TFTP-сервером.

Переконайтеся, що є доступ до мережевого TFTP-сервера. Пропінгуйте TFTP-сервер для перевірки підключення.

Крок 2. Перевірка розміру зображення у флеш-пам'яті.

Переконайтеся, що на сервері TFTP досить дискового простору для розміщення образу програмного забезпечення Cisco IOS. Використовуйте команду show flash0: на маршрутизаторі, щоб визначити розмір файлу образу Cisco IOS.

Крок 3. Копіювання зображення на TFTP-сервер.

Скопіюйте зображення на TFTP-сервер за допомогою команди **copy source-url destination-url.** Після введення команди з використанням

зазначених вихідних і цільових URL-адрес користувачеві пропонується ввести ім'я вихідного файлу, IP-адреса віддаленого хоста і ім'я кінцевого файлу. Як правило, ви натискаєте Enter, щоб прийняти ім'я файлу джерела в якості імені файлу призначення. Передача почнеться (рисунок 3.16).

Рисунок 3.16 – Використання команди **copy source-url destination-url**

Команда завантаження системи

Щоб оновити скопійований образ IOS після збереження цього образу у флеш-пам'яті маршрутизатора, налаштуйте маршрутизатор на використання нового способу під час завантаження за допомогою команди **boot system**, як показано на рисунку 3.17. Збережіть конфігурацію. Перезавантажте маршрутизатор, щоб завантажити маршрутизатор з новим образом.

Рисунок 3.17 – Використання команди **boot system**

Під час запуску код початкового завантаження аналізує файл конфігурації запуску в NVRAM для команд завантажувального системи, які вказують ім'я та розташування образу програмного забезпечення Cisco IOS для завантаження. Кілька команд системи завантаження можуть бути введені послідовно для забезпечення різних варіантів отказоустойчивого плану завантаження.

Якщо в конфігурації немає команд завантажувального системи, маршрутизатор за замовчуванням знаходить перший дійсний образ Cisco IOS у флеш-пам'яті і запускає його. Після завантаження маршрутизатора, щоб переконатися, що новий образ завантажений, використовуйте команду **show version.**

ЛЕКЦІЯ 2
ПРОТОКОЛ РЕЗЕРВУВАННЯ ПЕРШОГО ПЕРЕХОДУ FHRP

2.1. Призначення, властивості протоколу FHRP

Існує проблема виходу з ладу маршрутизатора, що є шлюзом за замовчуванням. У разі збою маршрутизатора або інтерфейсу маршрутизатора (який служить шлюзом за замовчуванням) вузли, налаштовані за допомогою цього шлюзу, ізолюються від зовнішніх мереж. У комутованої мережі кожен клієнт отримує тільки один шлюз за замовчуванням. Неможливо використовувати другий шлюз, навіть якщо існує другий шлях для передачі пакетів з локального сегмента. Жоден з хостів не зможе відправляти повідомлення за межі локальної мережі. Буде потрібно якийсь час, щоб цей шлюз знову запрацював.

Потрібен механізм для забезпечення альтернативних шлюзів за замовчуванням в комутованих мережах, де два або більше маршрутизатора підключені до одних і тих же VLAN. Цей механізм забезпечується протоколами резервування першого переходу - First Hop Redundancy Protocols (FHRPs).

Топологія фізичної мережі на рисунку 3.18 показує два комутатора, маршрутизатори, ПК і сервер. Маршрутизатор R1 відповідає за маршрутизацію пакетів від ПК1. Якщо R1 стає недоступним, протоколи маршрутизації можуть динамічно сходитися. R2 тепер направляє пакети із зовнішніх мереж, які пройшли б через R1. Однак трафік з внутрішньої мережі, пов'язаної з R1, включаючи трафік з робочих станцій, серверів і принтерів, налаштованих з R1 в якості шлюзу, як і раніше відправляється на R1 і відкидається.

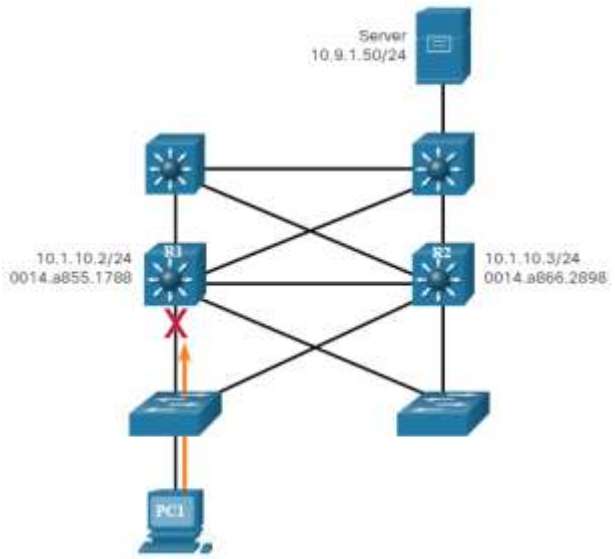


Рисунок 3.18 – Топологія фізичної мережі

Примітка. При розгляді резервування маршрутизатора не існує функціональної різниці між комутатором рівня 3 і маршрутизатором на рівні розподілу. На практиці комутатор рівня 3 зазвичай виступає в якості шлюзу для кожної VLAN в комутованій мережі. Це опис зосереджено на функціональності маршрутизації, незалежно від використовуваного фізичного пристрою.

Кінцеві пристрої зазвичай настроюються з одною IPv4-адресою для шлюзу. Ця електронна адреса не змінюється при зміні топології мережі. Якщо цей IPv4-адрес шлюзу за замовчуванням не може бути досягнутий, локальний пристрій не може відправляти пакети з сегмента локальної мережі і відключається від інших мереж. Навіть якщо існує резервний маршрутизатор, який може служити шлюзом за замовчуванням для цього сегмента, не існує динамічного методу, за допомогою якого ці пристрої можуть визначати адресу нового шлюзу.

Примітка. Пристрої IPv6 отримують адресу шлюзу динамічно з оголошення маршрутизатора ICMPv6. Однак при використанні протоколу FHRP пристрої IPv6 виграють завдяки більш швидкому переключенню на новий шлюз.

У протоколі FHRP як шлюз для робочих станцій в певному сегменті налаштований IPv4-адрес віртуального маршрутизатора. Коли кадри відправляються з хост-пристроїв на шлюз за замовчуванням, хости використовують ARP для визначення MAC-адреси, пов'язаного з IPv4-адресою шлюзу. Дозвіл ARP повертає MAC-адресу віртуального маршрутизатора. Кадри, відправлені на MAC-адресу віртуального маршрутизатора, можуть потім фізично оброблятися активним в даний момент маршрутизатором в групі віртуальних маршрутизаторів (рисунок 3.19).

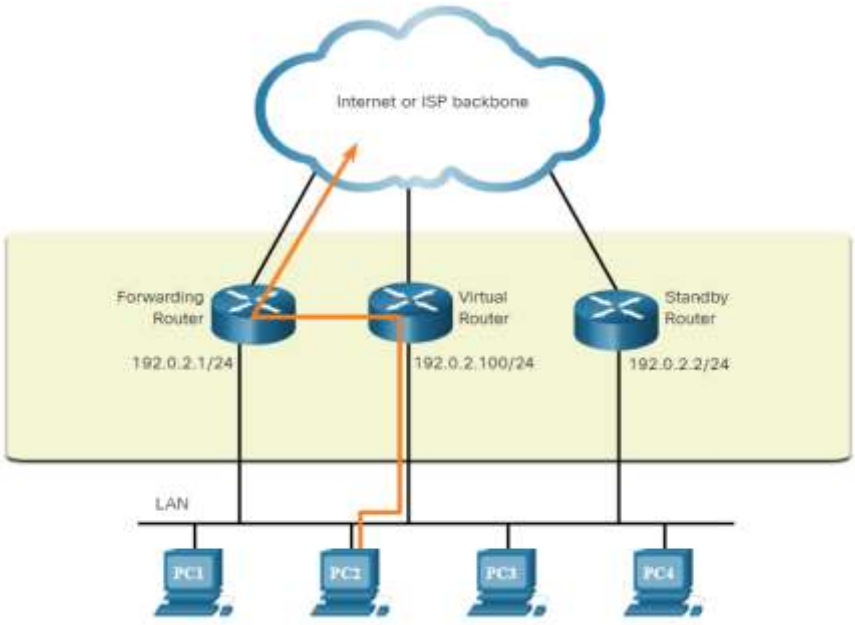


Рисунок 3.19 – Застосування віртуальних маршрутизаторів

Протокол використовується для ідентифікації двох або більше маршрутизаторів як пристроїв, що відповідають за обробку кадрів, що відправляються на MAC-адресу або IP-адреса одного віртуального маршрутизатора. Хост-пристрої відправляють трафік на адресу віртуального маршрутизатора. Фізичний маршрутизатор, який пересилає цей трафік, не важлива для хост-пристроїв.

Протокол резервування забезпечує механізм для визначення, який маршрутизатор повинен відігравати активну роль в пересиланні трафіку. Він також визначає, коли роль переадресації повинен прийняти резервний маршрутизатор. Перехід від одного маршрутизатора пересилання до іншого неважливий для кінцевих пристроїв. Така здатність мережі динамічно відновлюватися після збою пристрою, який виступає в якості шлюзу, називається резервуванням першого переходу.

Кроки для аварійного перемикання маршрутизатора

При збої активного маршрутизатора протокол резервування переводить резервний маршрутизатор в нову роль активного маршрутизатора, як показано на рисунку 3.20. Це кроки, які відбуваються при збої активного маршрутизатора:

1. Резервний маршрутизатор перестає бачити привітальні повідомлення від ретранслює маршрутизатора.

2. Резервний маршрутизатор приймає на себе роль перенаправляє маршрутизатора.

3. Оскільки новий маршрутизатор пересилання приймає як IPv4, так і MAC-адресу віртуального маршрутизатора, хост-пристрої не бачать збоїв в обслуговуванні.

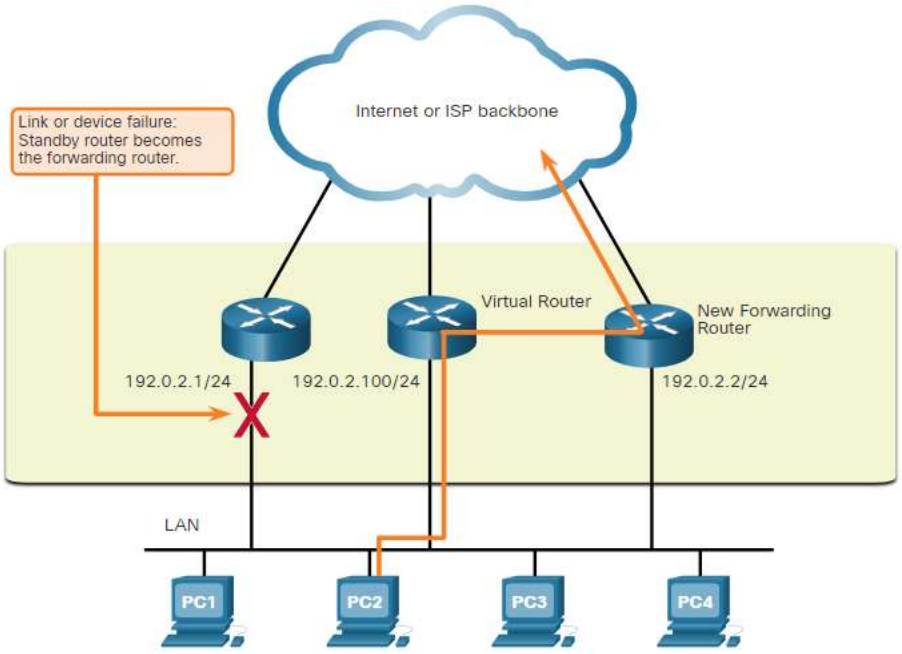


Рисунок 3.20 – Аварійне перемикання маршрутизатора

2.2. Різновиди протоколів FHRP

Далі перераховані всі варіанти, доступні для реалізації FHRP.

Протокол маршрутизатора з гарячим резервуванням (Hot Standby Router Protocol, HSRP)

HRSP є пропрієтарним FHRP, розробленим Cisco, який забезпечує прозоре перемикання при відмові пристрою IPv4 першого переходу. HSRP забезпечує високу доступність мережі, забезпечуючи резервування маршрутизації на першому переході для вузлів IPv4 в мережах, налаштованих з адресою шлюзу IPv4. HSRP використовується в групі маршрутизаторів для вибору активного пристрою і резервного пристрою. У групі інтерфейсів пристроїв активний пристрій - це пристрій, який використовується для маршрутизації пакетів, резервне пристрій - це пристрій, який вступає в роботу при відмові активного пристрою або при виконанні встановлених умов. Функція резервного маршрутизатора HSRP полягає в тому, щоб відстежувати робочий стан групи HSRP і швидко брати на себе відповідальність за пересилку пакетів в разі збою активного маршрутизатора.

HSRP для IPv6

Це власний FHRP від Cisco, який забезпечує ті ж функції HSRP, але в середовищі IPv6. Група HSRP IPv6 має віртуальний MAC-адресу, отриманий з номера групи HSRP, і віртуальний локальний IPv6-адреса, отриманий з віртуального MAC-адреси HSRP. Періодичні оголошення маршрутизатора (RA) відправляються для віртуального локального адреси каналу IPv6 HSRP, коли група HSRP активна. Коли група стає неактивною, ці RA зупиняються після відправки остаточного RA.

Протокол резервування віртуальних маршрутизаторів версії 2 (Virtual Router Redundancy Protocol, VRRPv2)

Це загальнодоступний протокол, який динамічно розподіляє відповідальність за один або кілька віртуальних маршрутизаторів на маршрутизатори VRRP в локальній мережі IPv4. Це дозволяє декільком маршрутизаторів в каналі множинного доступу використовувати один і той же віртуальний адреса IPv4. Маршрутизатор VRRP налаштований для запуску протоколу VRRP в поєднанні з одним або декількома іншими маршрутизаторами, підключеними до локальної мережі. У конфігурації VRRP один маршрутизатор вибирається в якості майстра віртуального маршрутизатора, а інші маршрутизатори виступають в якості резервних копій на випадок збою майстри віртуального маршрутизатора.

VRRPv3

Дозволяє підтримувати адреси IPv4 і IPv6. VRRPv3 працює в мультивендорної середовищах і є більш масштабованим, ніж VRRPv2.

Протокол балансування навантаження шлюзу (Gateway Load Balancing Protocol GLBP)

Це власний протокол FHRP, розроблений компанією Cisco, який захищає трафік даних від несправного маршрутизатора або каналу, такого як HSRP і VRRP, а також дозволяє балансувати навантаження (також відому як розподілом навантаження) між групою резервних маршрутизаторів.

GLBP для IPv6

Це пропріетарний FHRP від Cisco, який забезпечує ті ж функціональні можливості GLBP, але в середовищі IPv6. GLBP для IPv6 забезпечує автоматичне резервне копіювання маршрутизатора для хостів IPv6, налаштованих з одним шлюзом за замовчуванням в локальній мережі. Кілька маршрутизаторів першого переходу в локальній мережі об'єднуються, щоб запропонувати один віртуальний маршрутизатор IPv6 першого переходу, одночасно розподіляючи навантаження пересилання пакетів IPv6.

Протокол виявлення маршрутизатора ICMP (Router Discovery Protocol, IRDP)

Зазначений в RFC 1256 протокол IRDP є застарілим рішенням FHRP. IRDP дозволяє хостам IPv4 знаходити маршрутизатори, які забезпечують підключення IPv4 до інших (нелокальним) IP-мереж.

2.3. Пріоритети, стан і робота маршрутизаторів з протоколом FHRP

HSRP протокол реалізований поверх стека протоколів TCP / IP, для доставки службової інформації використовується протокол UDP. Маршрутизатор або маршрутизовані комутатори, на яких налаштований і функціонує протокол HSRP, в рамках обміну службовою інформацією використовують так звані пакети вітання (hello packets). У свою чергу, дані пакети відправляються на IP-адреса групової розсилки 224.0.0.2 (HSRP Version 1) або на 224.0.0.102 (HSRP Version 2) по протоколу UDP на порт 1985.

HSRP забезпечує високу доступність мережі, забезпечуючи резервування маршрутизації в першому переході для IP-хостів у мережах, налаштованих з використанням IP-адреси шлюзу за замовчуванням. HSRP використовується в групі маршрутизаторів для вибору активного пристрою і резервного пристрою.

Роль активного і резервного маршрутизаторів визначається під час процесу вибору HSRP. За умовчанням як активного маршрутизатора обраний маршрутизатор з найбільшим за чисельністю адресою IPv4. Однак завжди краще контролювати, як ваша мережа буде працювати в нормальних умовах, ніж залишати це на волю випадку.

Пріоритет HSRP (HSRP Priority) може використовуватися для визначення активного маршрутизатора. Маршрутизатор з найвищим пріоритетом HSRP стане активним маршрутизатором. За замовчуванням пріоритет HSRP дорівнює 100. Якщо пріоритети рівні, як активного маршрутизатора вибирається маршрутизатор з найвищим цифровим адресою IPv4.

Щоб налаштувати маршрутизатор як активний маршрутизатор, використовують команду інтерфейсу standby priority. Діапазон пріоритету HSRP становить від 0 до 255.

HSRP заміщення

За замовчуванням після того, як маршрутизатор стає активним, він залишиться активним, навіть якщо інший маршрутизатор підключиться до мережі з більш високим пріоритетом HSRP.

Щоб новий процес вибору HSRP відбувався при підключенні маршрутизатора з більш високим пріоритетом, необхідно включити пріоритетне перемикання за допомогою команди інтерфейсу **standby preempt.**

Заміщення - це здатність маршрутизатора HSRP ініціювати процес переобрання. При включеному витіснення роль активного маршрутизатора буде виконувати маршрутизатор, підключений до мережі з більш високим пріоритетом HSRP.

Попередня установка дозволяє маршрутизатора ставати активним маршрутизатором, тільки якщо він має більш високий пріоритет. Маршрутизатор, включений для витіснення, з рівним пріоритетом, але з більш високим IPv4-адресою, що не буде витісняти активний маршрутизатор.

На рисунку 3.21 показана топологія в якій R1 був налаштований з пріоритетом HSRP 150, в той час як R2 має пріоритет HSRP за замовчуванням 100. Заміщення було включено на R1. R1 є активним маршрутизатором завдяки вищому пріоритету, а R2 є резервним маршрутизатором. Через збій харчування, що впливає тільки на R1, активний маршрутизатор більше не доступний, а резервний маршрутизатор R2 приймає на себе роль активного маршрутизатора. Після відновлення електропостачання R1 знову включається. Оскільки R1 має більш високий пріоритет і пріоритетне заміщення включено, це викличе новий процес виборів і R1 знову прийме роль активного маршрутизатора, а R2 повернеться до ролі резервного маршрутизатора.

Примітка. Якщо пріоритетне заміщення відключено, маршрутизатор, який завантажується першим, стане активним маршрутизатором, якщо під час процесу вибору іншихмаршрутизаторів в мережі не буде.

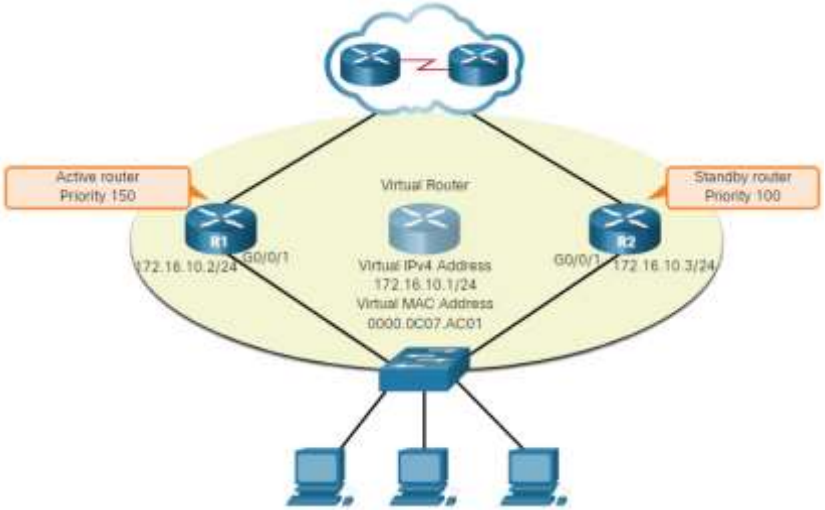


Рисунок 3.21 – Топологія мережі з заміщенням

Стани і таймери HSRP

Коли інтерфейс маршрутизатора налаштований з HSRP маршрутизатор відправляє і приймає пакети вітання HSRP, щоб почати процес визначення, яке стан він прийме в групі HSRP.

У таблиці 3.1 наведені стани HSRP.

Таблиця 3.1

Назва стану HSRP	**Опис стану HSRP**
Початкове **Initial**	Цей стан вводиться при зміні конфігурації або коли інтерфейс вперше стає доступним.
Вивчення **Learn**	Маршрутизатор не визначив віртуальний IP-адреса і ще не бачив вітальне повідомлення від активного маршрутизатора. У цьому стані маршрутизатор очікує відповіді від активного маршрутизатора.
Прослуховування **Listen**	Маршрутизатор знає віртуальний IP-адреса, але він не є ні активним, ні резервним маршрутизатором. Він слухає привітальні повідомлення від цих маршрутизаторів.
Оголошення **Speak**	Маршрутизатор періодично відправляє вітальні повідомлення і бере активну участь у виборі активного і / або резервного маршрутизатора.
Режим очікування **Standby**	Маршрутизатор є кандидатом на те, щоб стати наступним активним маршрутизатором, і періодично відправляє вітальні повідомлення.

Активні і резервні маршрутизатори HSRP відправляють привітальні пакети на груповий адресу групи HSRP за замовчуванням кожні 3 секунди (рисунок 3.22). Резервний маршрутизатор стане активним, якщо через 10 секунд він не отримає вітальне повідомлення від активного маршрутизатора. Можна зменшити ці настройки таймера, щоб прискорити аварійне перемикання або переривання. Проте, щоб уникнути збільшення завантаження ЦП і непотрібних змін стану очікування не варто встановлювати таймер вітання менше 1 секунди або таймер утримання менше 4 секунд.

<table>
<tr><td>0</td><td></td><td>7</td><td>15</td><td>23</td></tr>
<tr><td>Version</td><td>Type</td><td>Virtual Rtr ID</td><td>Priority</td><td>Count IP Addrs</td></tr>
<tr><td colspan="2">Auth Type</td><td>Advet Int</td><td colspan="2">Checksum</td></tr>
<tr><td colspan="5">IP Address (1)</td></tr>
<tr><td colspan="5">…</td></tr>
<tr><td colspan="5">IP Address (n)</td></tr>
<tr><td colspan="5">Authentication Data (1)</td></tr>
<tr><td colspan="5">Authentication Data (2)</td></tr>
</table>

Рисунок 3.22 – Структура пакета

Команди налаштування протоколу HSRP:

– standby **номер_групи** ip **ip-адреса** – вказує адресу ip-адреса віртуального маршрутизатора в зазначеній групі;

– standby version **версія_протокола** – вказує версію протоколу 1 або 2;

– standby **номер_групи** priority **значення_пріорітету** – вказує пріоритет маршрутизатора в зазначеній групі;

– standby **номер_групи** preempt – дозволяє перехоплення функцій якщо пріоритет вище ніж у активного маршрутизатора;

– standby **номер_групи** track **ім'я_інтерфейса_пріоритету** – знижує значення пріоритету маршрутизатора на зазначену величину пріоритету якщо інтерфейс недоступний. Значення відновиться якщо інтерфейс стане доступний;

– standby **номер_групи** timers **hellotime_сек holdtime_сек** – задає значення таймерів hellotime і holdtime;

– standby **номер_групи** authentication **пароль** – пароль для доступу до цієї групи.

Приклад налаштування (рисунок 3.23).

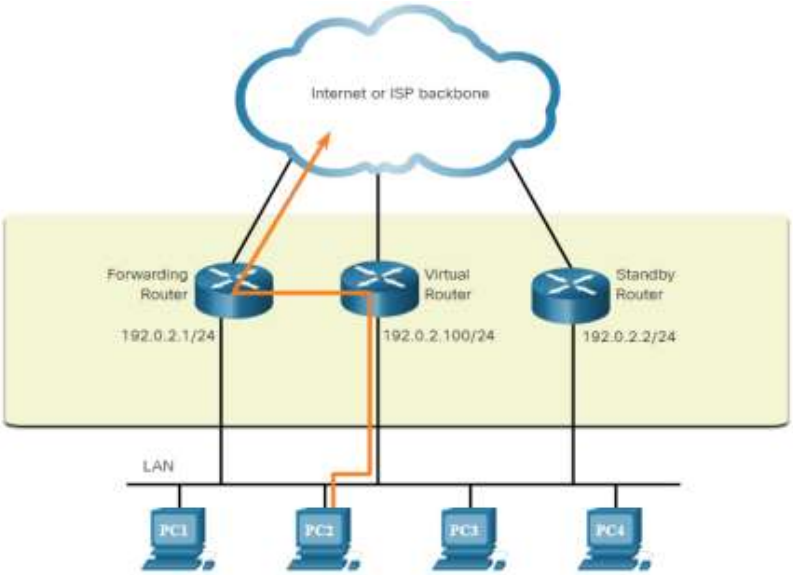


Рисунок 3.23 – Приклад налаштування

```
R1(config)# interface g0/1
R1(config-if)# standby version 2
R1(config-if)# standby 1 ip 192.0.2.100
R1(config-if)# standby 1 priority 150
R1(config-if)# standby 1 preempt

R3(config)# interface g0/0
R3(config-if)# standby version 2
R3(config-if)# standby 1 ip 192.0.2.100

R1# show standby
GigabitEthernet0/1 - Group 1 (version 2)
State is Active
4 state changes, last state change 00:00:30
Virtual IP address is 192.0.2.100
Active virtual MAC address is 0000.0C9F.F001
Local virtual MAC address is 0000.0C9F.F001 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 1.696 secs
Preemption enabled
Active router is local
Standby router is 192.0.2.2
Priority 150 (configured 150)
Group name is "hsrp-Gi0/1-1" (default)

R3# show standby
GigabitEthernet0/0 - Group 1 (version 2)
State is Standby
4 state changes, last state change 00:02:29
Virtual IP address is 192.0.2.100
Active virtual MAC address is 0000.0C9F.F001
Local virtual MAC address is 0000.0C9F.F001 (v2 default)
Hello time 3 sec, hold time 10 sec
Next hello sent in 0.720 secs
Preemption disabled
```

```
Active router is 192.0.2.1
MAC address is d48c.b5ce.a0c1
Standby router is local
Priority 100 (default 100)
Group name is "hsrp-Gi0/0-1" (default)


R1# show standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Gi0/1 1 150 P Active local 192.0.2.2 192.0.2.100

R3# show standby brief
P indicates configured to preempt.
|
Interface Grp Pri P State Active Standby Virtual IP
Gi0/0 1 100 Standby 192.0.2.1 local 192.0.2.100
```

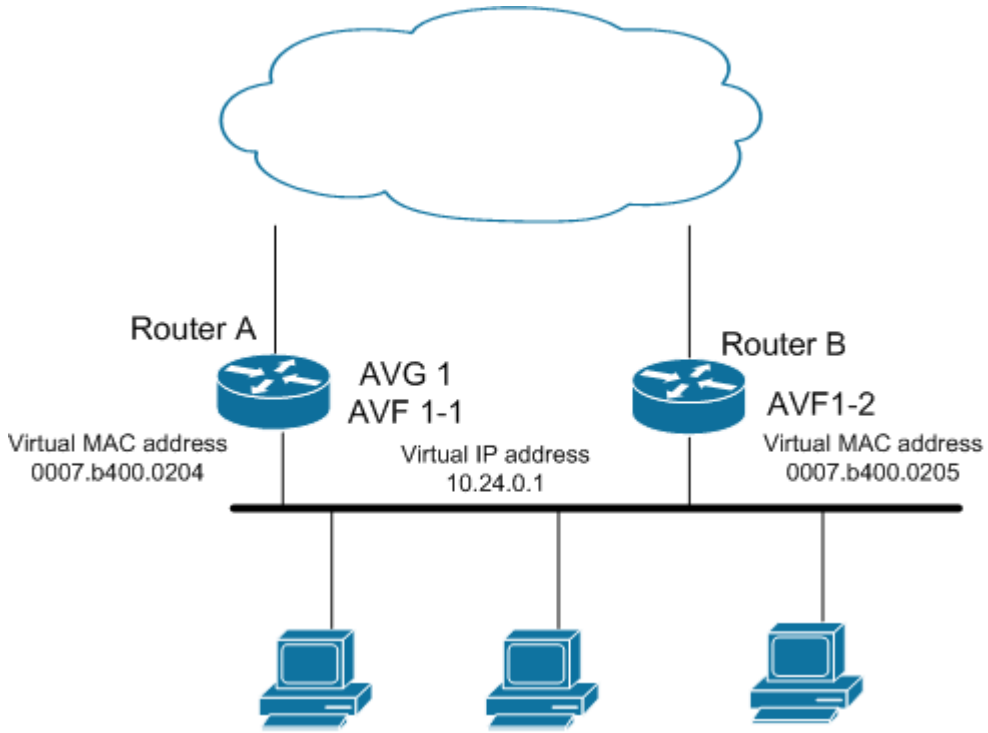
2.4. Балансування навантаження шлюза (GLBP)

GLBP працює аналогічно, але не ідентично іншим протоколам резервування шлюзу, такими як HSRP і VRRP.

Члени GLBP групи вибирають один шлюз який буде активним віртуальним шлюзом **active virtual gateway (AVG)** для цієї групи. Інші члени групи забезпечують резервування для AVG в разі якщо AVG стане недоступним. AVG призначає віртуальний MAC адреса для кожного члена GLBP групи. Кожен член групи бере участь в передачі пакетів, використовуючи віртуальний MAC адресу, виданий AVG. Цих членів групи називають **active virtual forwarders (AVFs)**. AVG відповідальний за видачу відповідей по протоколу **Address Resolution Protocol (ARP)** на запити до віртуального IP-адресою. Розподіл навантаження досягається тим що AVG відповідає на ARP запити використовуючи різні віртуальні MAC-адреси.

На рисунку 3.24 маршрутизатор A є AVG для GLBP групи, і відповідальний за віртуальний IP-адреса 10.24.0.1. Маршрутизатор A так само є AVF для віртуального MAC адреси 0007.b400.0204. Маршрутизатор B член тієї ж GLBP групи і призначений AVF для віртуального MAC адреси 0007.b400.0205. На клієнтах встановлюється шлюз з IP-адресою 10.24.0.1 і MAC адресою шлюзу 0007.b400.0204. У той час як на іншому клієнті MAC-адресу шлюзу за замовчуванням буде 0007.b400.0205 і таким чином маршрутизатор A буде розподіляти навантаження з маршрутизатором B.

GLBP підтримує до 4 маршрутизаторів в групі і до 1024 груп. Маршрутизатор відправляють один одному повідомлення hello кожні 3 секунди. Повідомлення відправляються на адресу 224.0.0.102, UDP порт 3222 (відправника і одержувача).



Рисунко 3.24 – Топологія мережі з балансуванням навантаження

GLBP Gateway Priority визначає роль, яку кожен маршрутизатор AVF грає в групі. Тобто за допомогою цієї властивості можна визначити послідовність вибору нового AVG, якщо старий AVG стане недоступним. Пріоритет можна визначити на кожному маршрутизаторі значенням від 1 до 255 командою: **glbp priority**. Маршрутизатор з великим пріоритетом стає AVG.

За замовчуванням схема вибору AVG тільки на основі пріоритету вимкнена. Запасний AVF стане AVG тільки якщо поточний AVG стане недоступним. Що б дозволити вибори AVG на основі пріоритету потрібно ввести команду: **glbp preempt**.

GLBP підтримує такі режими балансування навантаження:

– **None** – режим, при якому комутатор не забезпечує балансування навантаження. На всі запити клієнтів він відповідає своїм MAC-адресою. Другий комутатор починає роботу тільки після того як основний комутатор (AVG) вийде з ладу або стане недоступним.

– **Weighted load-balancing** – балансування навантаження проводиться відповідно до ваги кожного комутатора. Вага комутатора призначається адміністратором на кожному комутаторі окремо. Наприклад якщо в GLBP групі два комутатора, у AVG вага 70, а у AVF 140, то навантаження буде розподілятися 1: 2. Іншими словами з трьох отриманих запитів на MAC-адресу AVG один раз відповість своїм MAC-адресою і двічі MAC-адресою AVF комутатора.

– **Host-dependent load-balancing** – цей режим використовується в разі якщо є необхідність в реалізації трансляції адрес Network Address Translation (NAT), так як цей режим гарантує повернення клієнту того ж MAC-адреси AVF комутатора, який він використовував раніше і отже NAT

сесія у клієнта не переривається. Клієнти будуть отримувати ті ж MAC-адреси AVF до тих пір, поки кількість комутаторів в GLBP групі не зміниться.

– **Round-robin load-balancing** – режим використовується за умовчанням. В цьому режимі AVG видає MAC-адреси AVF поперемінно.

Налаштування GLBP на маршрутизаторах Cisco (рисунок 3.25):

– включення GLBP на інтерфейсі:

glbp <group> ip [ip-address [secondary]]

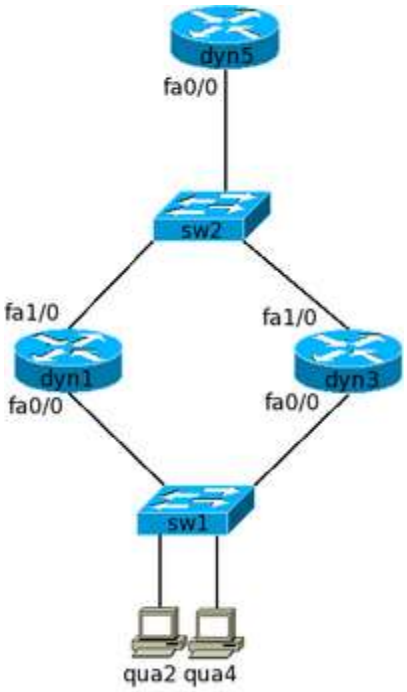


Рисунок 3.25 – Приклад налаштування

– включення режиму preempt GLBP:

У GLBP є два режими preempt:

– для **AVG** - за замовчуванням відключений,

– для **AVF** - за замовчуванням включений, з затримкою 30 секунд.

За замовчуванням режим preempt для **AVG** відключений. Тобто, backup virtual gateway може стати AVG тільки якщо поточний AVG вийде з ладу.

Включення режиму preempt для AVG:

dyn1(config-if)# glbp 1 preempt

Включення режиму preempt для AVF:

dyn1(config-if)# glbp 1 forwarder preempt [delay minimum <seconds>]

– налаштування методу балансування навантаження між маршрутизаторами (за замовчуванням round-robin):

```
dyn1(config-if)# glbp 1 load-balancing <host-dependent | round-robin |
weighted>
```

– зміна методу балансування навантаження:

```
dyn1(config-if)# glbp 1 load-balancing host-dependent
```

– вимкнення балансування навантаження:

```
dyn1(config-if)# no glbp 1 load-balancing
```

– налаштування інтервалу між відправкою AVG повідомлень hello в групі GLBP:

```
dyn1(config-if)# glbp <group> timers [msec] <hellotime> [msec] <holdtime>
dyn1(config-if)# glbp <group> timers redirect <redirect> <timeout>
```

Параметри команди:

– redirect - налаштовує інтервал протягом якого AVG продовжує перенаправляти клієнтів AVF. За замовчуванням 600 секунд (10 хвилин);

– timeout - вказує інтервал в секундах до того як secondary virtual forwarder стане invalid. За замовчуванням 14,400 секунд (4 години).

Хоча діапазон значень параметра redirect дозволяє використовувати значення 0, фактично воно не повинно використовуватися. Це призведе до того, що таймер redirect не має терміну дії і, в разі виходу з ладу маршрутизатора, хости все одно будуть відправлятися на нього.

– Налаштування Object Tracking і вказівка об'єкта, який буде впливати на вагу GLBP, якщо інтерфейс вимикається, то вага зменшується на 11 (за замовчуванням на 10):

```
dyn1(config)# track 1 interface FastEthernet1/0 line-protocol
dyn1(config-if)# glbp 1 weighting track 1 decrement 11
```

– Налаштування порогових значень ваги, які регулюють чи маршрутизатор виконувати роль GLBP gateway:

```
dyn1(config-if)# glbp 1 weighting track 1 decrement 11
```

Для даного прикладу, початкове значення 200. Якщо інтерфейс fa1 / 0 вимикається, то значення стає 189. Так як воно менше, ніж значення **lower**, то

маршрутизатор не може виконувати роль active forwarder. Коли інтерфейс включиться, то значення стане знову 200. Так як це більше ніж значення **upper**, то маршрутизатор знову стає active forwarder.

За допомогою цих порогових значень можна прив'язувати певні значення ваг таким чином, щоб, наприклад, якщо два інтерфейси не доступні (з альтернативними шляхами до мережі), то тоді маршрутизатор не виконуватиме роль active forwarder.

– Налаштування GLBP Client Cache:

```
dyn1(config-if)# glbp 1 client-cache
```

За замовчуванням функція GLBP Client Cache відключена. Після включення функції AVG починає зберігати у себе інформацію про те які хости використовують який gateway.

– Перегляд інформації про GLBP Client Cache (зберігається тільки на AVG):

```
dyn1# show glbp detail
```

– Перегляд короткої інформації в групах:

```
dyn1# show glbp brief
```

– перегляд інформації про всі включені групи GLBP:

```
dyn1# show glbp
```

ЛЕКЦІЯ 3
ПРОТОКОЛИ КОМУТОВАНОЇ МЕРЕЖІ З АГРЕГАЦІЄЮ ЛІНІЙ

3.1. Принцип агрегації ліній EtherChannel

Якщо мережа включає в себе резервні комутатори та лінії, то для запобігання петель 2-го рівня налаштовується якась версія протоколу STP. Однак якщо виникає необхідність використовувати велику пропускну здатність в надлишкової мережі, то може допомогти протокол EtherChannel, який об'єднує кілька ліній між комутаторами в єдиний канал. Ці канали об'єднують паралельні лінії, забезпечуючи збільшену пропускну здатність, при цьому STP запобігатиме петлі. Є два протоколи EtherChannel - PAgP і LACP.

Однак кілька паралельних ліній, включених між комутаторами, будуть блокуватися протоколом Spanning Tree Protocol (STP), який за замовчуванням включений на пристроях рівня 2, таких як комутатори Cisco, для запобігання петель 2-го рівня (рисунок 3.26).

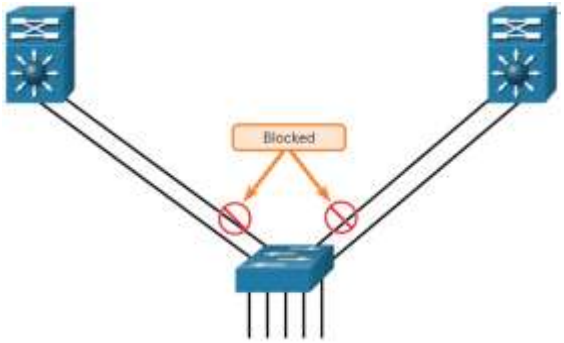


Рисунок 3.26 – Зображення прикладу агрегації ліній EtherChannel

Потрібно технологія агрегації ліній, яка дозволяє створювати паралельні лінії між пристроями, які не будуть блокуватися STP. Ця технологія відома як EtherChannel.

EtherChannel, **PortChannel** — технологія агрегації каналів, що була розроблена компанією Cisco Systems. Технологія дозволяє об'єднувати декілька фізичних каналів Ethernet в один логічний (віртуальний порт, який називається PortChannel) для збільшення пропускної здатності та підвищення надійності з'єднання. Можливо створити декілька окремих PortChannel на одному комутаторі.

Технологія EtherChannel надає ряд переваг:

1. Більшість завдань по налаштуванню можна виконувати на загальному інтерфейсі EtherChannel, а не на кожному окремому порту, забезпечуючи узгодженість конфігурації по всіх каналах.

2. EtherChannel спирається на існуючі порти комутатора. Немає необхідності докуповувати обладнання для більш швидкого з'єднання і забезпечення великої пропускної здатності (рисунок 3.27).

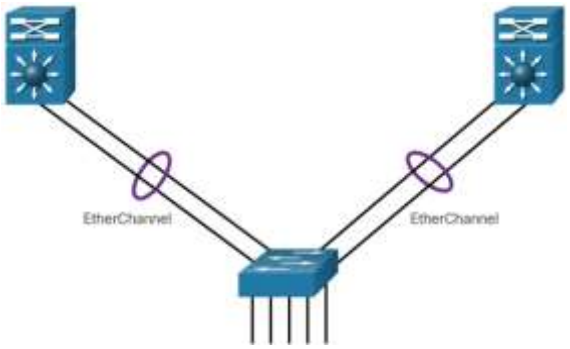


Рисунок 3.27 – Приклад формування EtherChannel

3. Балансування навантаження відбувається між лініями, які є частиною одного EtherChannel. Залежно від апаратної платформи може бути реалізований один або кілька методів розподілу навантаження. Ці методи включають розподіл навантаження по фізичних каналах, з урахуванням MAC-адреси джерела і призначення або з урахуванням IP-адреси джерела і призначення.

4. EtherChannel створює агрегацію, яка розглядається як одне логічне ланка. Коли між двома комутаторами існує кілька каналів EtherChannel, STP може заблокувати один з каналів, щоб запобігти петлі 2-го рівня. Коли STP блокує один з паралельних каналів, він блокує весь EtherChannel (всі порти, що належать цьому каналу EtherChannel). Якщо ж є тільки один канал EtherChannel, то все фізичні лінії в EtherChannel залишаються активними, тому що STP їх бачить як одну (логічну) лінію.

5. EtherChannel забезпечує резервування, тому що загальна лінія розглядається як одне логічне з'єднання, при цьому відключення однієї фізичної лінії в каналі не призводить до зміни топології. Тому перерахунок сполучного дерева не потрібно. Припускаючи, що принаймні одна фізична зв'язок присутній; EtherChannel залишається працездатним, навіть якщо його загальна пропускна здатність зменшується через втрату зв'язку в EtherChannel.

Обмеження реалізації EtherChannel:

1. В одному EtherChannel не можуть бути змішані різні типи інтерфейсів, наприклад, Fast Ethernet і Gigabit Ethernet не можна змішувати.

2. Кожен EtherChannel може складатися не більше ніж з восьми сумісних портів Ethernet. EtherChannel забезпечує полнодуплексную смугу пропускання до 800 Мбіт / с (Fast EtherChannel) або 8 Гбіт / с (Gigabit EtherChannel) між двома комутаторами або комутатором і хостом.

3. Комутатор Cisco Catalyst 2960 в даний час підтримує до шести каналів EtherChannel. Однак у міру розробки нових IOS і зміни платформ деякі карти і платформи можуть підтримувати збільшення кількості портів в

каналі EtherChannel, а також підтримувати збільшення кількості каналів EtherChannel.

4. Конфігурація окремого порту в складі каналу EtherChannel повинна бути однаковою на обох пристроях. Якщо фізичні порти одного боку налаштовані як транки, фізичні порти іншого боку також повинні бути налаштовані як транки з тієї ж native VLAN. Крім того, всі порти в кожному каналі EtherChannel повинні бути налаштовані як комутовані порти.

5. Кожен EtherChannel має свій інтерфейс каналу логічного порту (рисунок 3.28) Конфігурація, що застосовується до інтерфейсу каналу порту, впливає на всі фізичні інтерфейси, які призначені цього інтерфейсу.

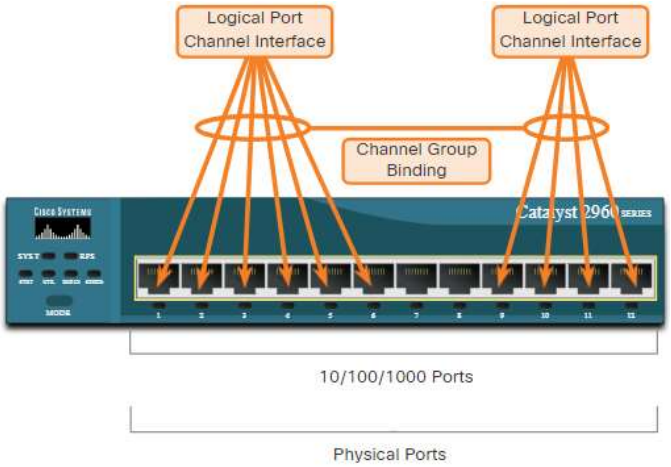


Рисунок 3.28 – Призначення інтерфейсів

Для того, щоб PortChannel міг існувати, необхідно, щоб всі вхідні в нього порти мали однакові параметри, а саме:

– Однакову швидкість (не можна створити portchannel, куди входили б, наприклад, FastEthernet0/1 і GigabitEthernet1/1 – або всі 10 Мбіт, або всі 100, або все – гігабіт і т.д.).

– Однакові налаштування дуплексу.

– Однакові налаштування VLAN-ів. У разі access портів – всі порти повинні бути в одному VLAN, в разі trunk портів – список дозволених VLAN (команда switchport trunk allowed vlan) так само повинен збігатися.

EtherChannel дає можливість об'єднувати від двох до восьми 100 Мбіт/с, 1 Гбіт/с або 10 Гбіт/с портів Ethernet (всі порти в каналі повинні мати однакову швидкість), який працює по витій парі або по оптоволокну, що дозволяє досягти результативної швидкості до 80 Гбіт/с. Додатково, від одного до восьми портів можуть бути неактивні і вмикатися в роботу при обриві з'єднання на одному з активних портів. За відсутності резервних портів, трафік автоматично розподіляється по з'єднанням що залишилися.

Канал може встановлюватися між маршрутизаторами, комутаторами і мережевими адаптерами на сервері (приклад на рисунок 3.29).

Усі мережеві адаптери, які є частиною каналу, отримують одну MAC-адресу, що робить канал прозорим для мережевих додатків. Балансування трафіку між портами виробляється на основі хеш-функції над MAC-адресою,

IP-адресою або TCP і UDP портом джерела або одержувача. Таким чином, в деяких несприятливих випадках, весь трафік може передаватися по одному фізичному з'єднанню.

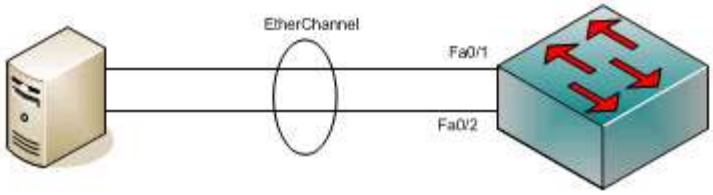


Рисунок 3.29 – EtherChannel між комутатором та сервером

При використанні протоколу STP разом з EtherChannel, усі з'єднання в каналі розглядаються як одне логічне і BPDU посилається тільки по одному з них. Спеціальний алгоритм дозволяє виявити невідповідності, коли один із комутаторів не налаштований для роботи з каналом.

При налаштуванні EtherChannel, порти на обох сторонах каналу додаються до нього вручну, або використовується протокол PAgP для автоматичної агрегації портів.

Коли два комутатора «домовляються» один з одним про використання між ними агрегованого каналу, застосовується один з двох протоколів: PAgP або LACP. PAgP - розроблявся спочатку cisco, а потім з'явився аналогічний відкритий стандарт LACP, який був оформлений у вигляді специфікації IEEE і використовується як на Catalist, так і на комутаторах інших виробників. Іншими словами, в сучасних реаліях найкраще використовувати LACP, так як він сумісний з усіма, на відміну від PAgP. У функціональному ж плані протоколи аналогічні. PortChannel може бути налаштований в одному з трьох режимів: On, Active і Passive (в LACP) або On, Auto, Desirable (в PAgP відповідно). Для того, щоб між комутаторами піднявся і заробив portchannel, необхідно, щоб обидві сторони були налаштовані в режимі On, або одна була в режимі Active, а інша – Passive.

3.2. Протокол автоузгодження EtherChannel

Канали EtherChannel можуть бути сформовані шляхом узгодження з використанням одного з двох протоколів: протоколу агрегації портів (Port Aggregation Protocol, PAgP) або протоколу керування агрегацією каналів (Link Aggregation Control Protocol, LACP). Ці протоколи дозволяють портам зі схожими характеристиками формувати канал за допомогою динамічного узгодження з сусідніми комутаторами.

Примітка. Також можливо налаштувати статичний або безумовний EtherChannel без PAgP або LACP.

Робота PAgP

PAgP (вимовляється як «Pag - P») - це власний протокол Cisco, який допомагає в автоматичному створенні каналів EtherChannel. Коли канал EtherChannel налаштований з використанням PAgP, пакети PAgP відправляються між портами з підтримкою EtherChannel для узгодження формування каналу. Коли PAgP ідентифікує відповідні Ethernet-канали, він групує ці канали в EtherChannel. Потім EtherChannel додається в сполучна дерево як один порт.

При включенні PAgP також управляє EtherChannel. Пакети PAgP відправляються кожні 30 секунд. PAgP перевіряє узгодженість конфігурації і управляє додаванням каналів і збоями між двома комутаторами. Це гарантує, що при створенні EtherChannel всі порти мають однаковий тип конфігурації.

Примітка. У EtherChannel обов'язково, щоб всі порти мали однакову швидкість, налаштування дуплексу і інформацію про VLAN. Будь-яка модифікація порту після створення каналу також змінює всі інші порти каналу.

PAgP допомагає створити канал EtherChannel, визначаючи конфігурацію кожного боку і забезпечуючи сумісність каналів, щоб при необхідності можна було включити канал EtherChannel. Режими для PAgP наступні:

On – цей режим змушує передавати інтерфейс в канал без PAgP. Інтерфейси, налаштовані у включеному режимі, не обмінюються пакетами PAgP.

PAgP desirable – цей режим PAgP переводить інтерфейс в активний стан узгодження, в якому інтерфейс ініціює переговори з іншими інтерфейсами, відправляючи пакети PAgP.

PAgP auto – цей режим PAgP переводить інтерфейс в стан пасивного узгодження, в якому інтерфейс відповідає на пакети PAgP, які він отримує, але не ініціює узгодження PAgP.

Режими повинні бути сумісні з кожного боку. Якщо одна сторона налаштована на роботу в автоматичному режимі, вона перекладається в пасивний стан, чекаючи, поки інша сторона ініціює узгодження EtherChannel. Якщо для іншого боку також встановлено значення auto, узгодження ніколи не починається, і EtherChannel не створюється. Якщо все режими відключені за допомогою команди no або режим не налаштований, EtherChannel відключається.

Режим включення вручну поміщає інтерфейс в EtherChannel без будь-яких погоджень. Це працює, тільки якщо інша сторона також включена. Якщо інша сторона налаштована на узгодження параметрів через PAgP, EtherChannel не створюється, оскільки сторона, для якої задано режим включення, не виконує узгодження.

Приклад налаштувань режиму PAgP

Розглянемо два комутатора на рисунку 3.30. Чи встановлять S1 і S2 EtherChannel за допомогою PAgP, залежить від налаштувань режиму на кожній стороні каналу.

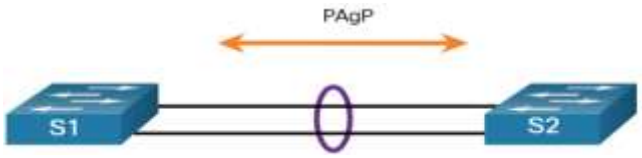


Рисунок 3.30 – Приклад налаштування

У таблиці 14 показана різна комбінація режимів PAgP на S1 і S2 і підсумковий результат встановлення каналу.

Таблиця 14

Режими PAgP

S1	S2	Channel Establishment
On	On	Yes
On	Desirable/Auto	No
Desirable	Desirable	Yes
Desirable	Auto	Yes
Auto	Desirable	Yes
Auto	Auto	No

Робота LACP

LACP є частиною специфікації IEEE (802.3ad), яка дозволяє об'єднувати декілька фізичних портів в єдиний логічний канал. LACP дозволяє комутатора автоматично погоджувати канал, відправляючи пакети LACP іншому комутатора. Розглянемо зміст відповідного кадру Ethernet від SW1. У Source-адреса він записує свій MAC-адресу, а в Destination-адреса (рисунок 3.31) мультікастового адреса 0180.C200.0002 (для протоколу PAgP використовується адреса 0100.0CCC.CCCC). Ця електронна адреса була зарезервована під протокол LACP. В інформаційному полі кадру передаються дані від LACP, це повідомлення використовується пристроями для багатьох цілей. Це синхронізація, збір, агрегація, перевірка активності і так далі, тобто у нього кілька функцій.

Перед початком взаємодії SW1 і SW2 вибирають собі віртуальний MAC-адресу. Зазвичай це найменший з наявних MAC-адрес на кожному з комутаторів (рисунок 3.32). І ось ці адреси вони будуть записувати в поля LACP (рисунок 3.33).

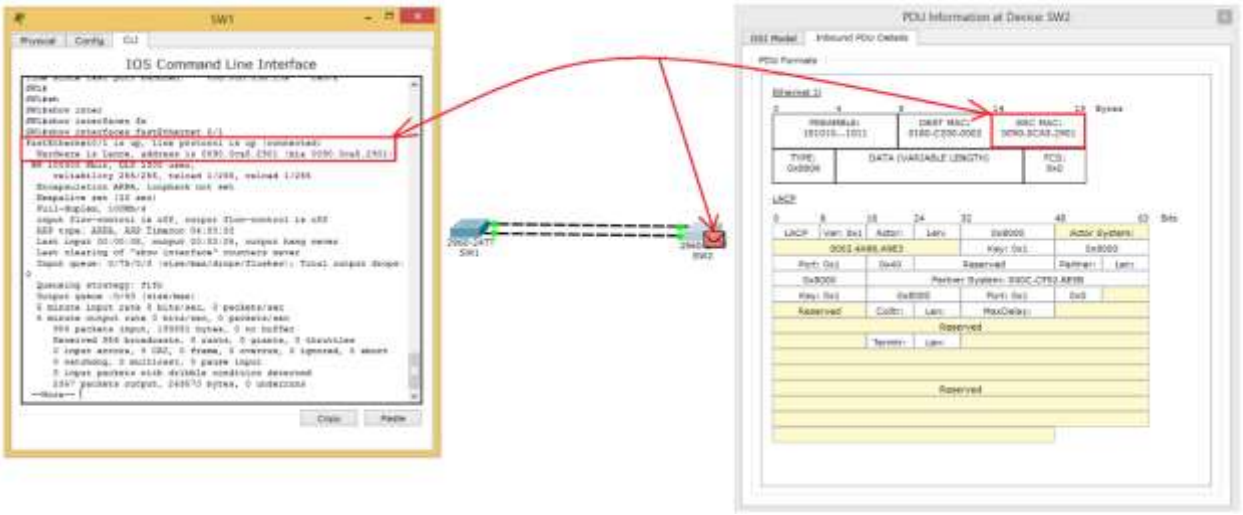


Рисунок 3.31 – Приклад налаштування

Рисунок 3.32 – Приклад налаштування

Він виконує функцію, аналогічну PAgP з Cisco EtherChannel. Оскільки LACP є стандартом IEEE, його можна використовувати для спрощення реалізації EtherChannels в мережах з обладнанням декількох виробників. На пристроях Cisco підтримуються обидва протоколи.

Примітка. LACP спочатку був визначений як IEEE 802.3ad. Однак LACP тепер визначено в більш новому стандарті IEEE 802.1AX для LAN і MAN.

LACP забезпечує ті ж переваги при веденні узгодження, що і PAgP. LACP допомагає створити канал EtherChannel, визначаючи конфігурацію кожного боку і перевіряючи їх сумісність, щоб при необхідності можна було включити канал EtherChannel.

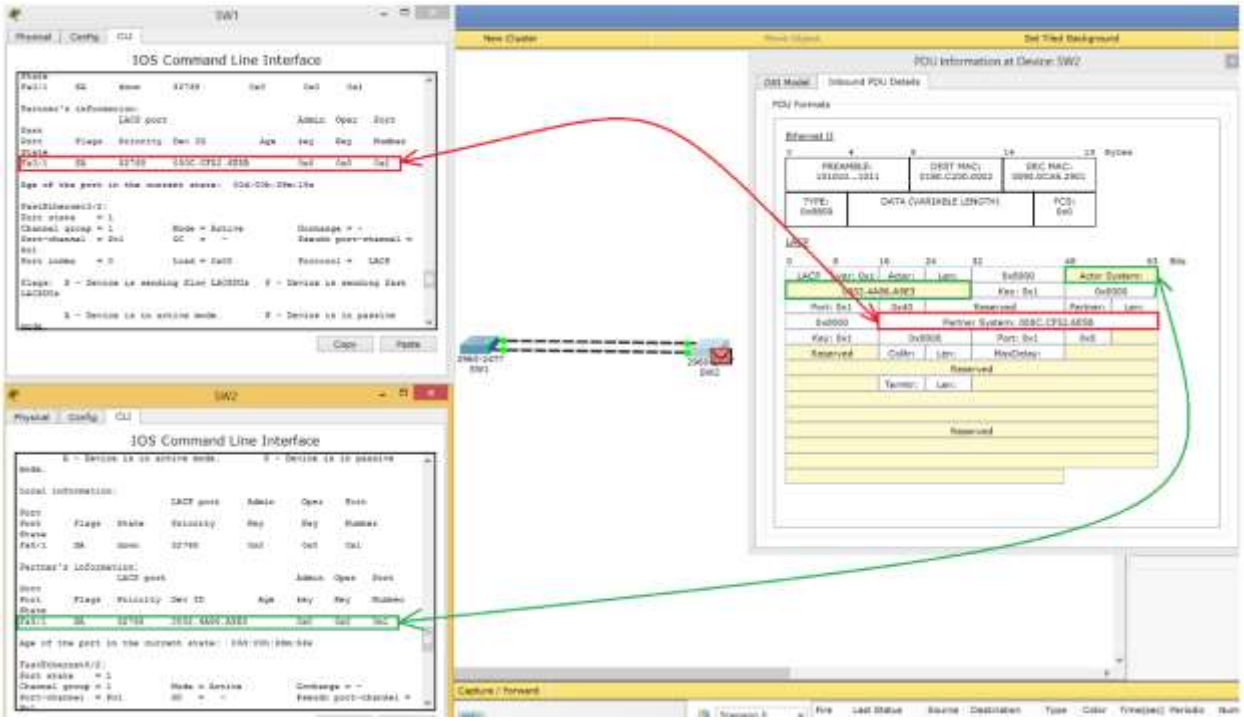


Рисунок 3.33 – Приклад налаштування

Режими для LACP наступні:

On – цей режим змушує передавати інтерфейс в канал без LACP. Інтерфейси, налаштовані у включеному режимі, не обмінюються пакетами LACP.

LACP active – цей режим LACP переводить порт в активний стан узгодження. У цьому стані порт ініціює переговори з іншими портами, відправляючи пакети LACP.

LACP passive – цей режим LACP переводить порт в стан пасивного узгодження. У цьому стані порт відповідає на пакети LACP, які він отримує, але не ініціює узгодження пакетів LACP.

Як і в разі PAgP, режими повинні бути сумісні з обох сторін, щоб канал EtherChannel міг сформуватися. Режим включення повторюється, оскільки він створює конфігурацію EtherChannel беззастережно, без динамічного узгодження PAgP або LACP.

LACP допускає вісім активних каналів, а також вісім резервних каналів. Резервна посилання стане активною в разі збою однієї з поточних активних посилань.

Приклад налаштувань режиму LACP

Розглянемо два комутатора на рисунку 3.34. Чи встановлять S1 і S2 EtherChannel з використанням LACP, залежить від налаштувань режиму на кожній стороні каналу.

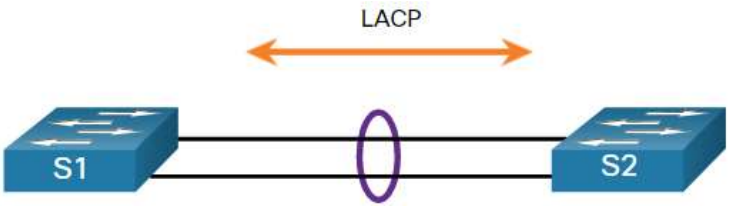


Рисунок 3.34 – Приклад налаштувань режиму LACP

У таблиці 2 показана різна комбінація режимів LACP на S1 і S2 і підсумковий результат встановлення каналу.

Таблиця 15

Режими LACP

S1	S2	Channel Establishment
On	On	Yes
On	Active/Passive	No
Active	Active	Yes
Active	Passive	Yes
Passive	Active	Yes
Passive	Passive	No

3.3. Порядок налаштування протоколів EtherChannel

Наступні рекомендації та обмеження корисні для настройки EtherChannel:

– Підтримка EtherChannel – все інтерфейси Ethernet повинні підтримувати EtherChannel без вимоги, щоб інтерфейси були фізично суміжними.

– Швидкість і дуплекс – налаштуйте все інтерфейси в EtherChannel для роботи з однаковою швидкістю і в одному дуплексному режимі.

– Відповідність VLAN – все інтерфейси в комплекті EtherChannel повинні бути призначені одній і тій же VLAN або налаштовані як транк.

– Діапазон VLAN – EtherChannel підтримує один і той же дозволений діапазон VLAN на всіх інтерфейсах транкінгового EtherChannel. Якщо допустимий діапазон VLAN не збігається, інтерфейси не формують EtherChannel, навіть якщо вони встановлені в auto або desirable режим.

На рисунку 3.35 показана конфігурація, яка дозволяє сформуватися EtherChannel між S1 і S2.

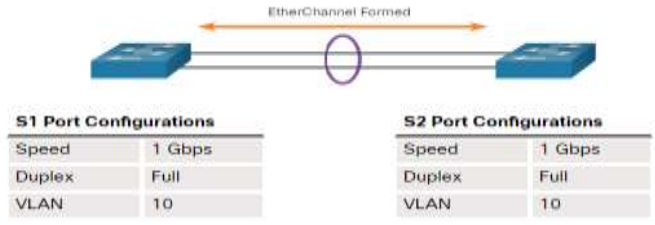


Рисунок 3.35 – Конфігурація, яка дозволяє сформувати EtherChannel між S1 і S2

EtherChannel формується, тільки коли настройки конфігурації збігаються на обох комутаторах.

Якщо ці параметри необхідно змінити, їх можна налаштувати в режимі настройки канального порту. Будь-яка конфігурація, яка застосовується до канального порту, також впливає на окремі інтерфейси. Однак конфігурації, які застосовуються до окремих інтерфейсів, не впливають на настройки канального порту. Тому внесення змін до конфігурації інтерфейсу, що є частиною каналу EtherChannel, може викликати проблеми сумісності інтерфейсу.

Канал порту може бути налаштований в режимі доступу, режим транка (найбільш поширеному) або на маршрутизації порту.

Приклад конфігурації LACP

EtherChannel відключений за замовчуванням і повинен бути налаштований. Топологія на рисунку 3.36 буде використана для демонстрації прикладу конфігурації EtherChannel з використанням LACP.

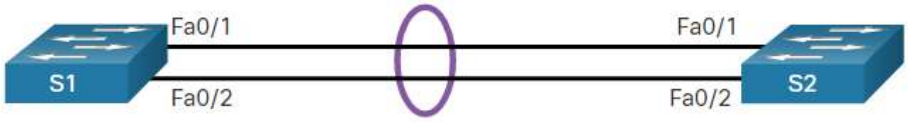


Рисунок 3.36 – Топологія для демонстрації прикладу конфігурації EtherChannel

Налаштування EtherChannel з LACP вимагає наступних трьох кроків (рисунок 3.37):

Крок 1. Вкажіть інтерфейси, які складають групу EtherChannel, за допомогою команди режиму глобальної конфігурації interface range interface. Ключове слово range дозволить вам вибрати кілька інтерфейсів і налаштувати їх всі разом.

Крок 2. Створіть інтерфейс каналу порту командою channel-group identifier mode active в режимі настройки діапазону інтерфейсів. Ідентифікатор вказує номер групи каналів. Ключові слова mode active активують це як конфігурацію LACP EtherChannel.

Крок 3. Щоб змінити налаштування ліній 2 рівня через інтерфейс канального порту, увійдіть в режим настройки інтерфейсу канального порту за допомогою команди interface port-channel + ідентифікатор інтерфейсу.

У прикладі на рис. 12 комутатор S1 налаштований з EtherChannel LACP. Канальний порт налаштований як магістральний інтерфейс з зазначеними дозволеними VLAN.

Перевірка EtherChannel

Завжди після налаштування пристрою в мережі необхідно перевірити його конфігурацію і, якщо є проблеми, їх потрібно буде локалізувати і

усунути. Далі розглянемо команди для перевірки, а також деякі поширені проблеми мережі з каналами EtherChannel і способи їх вирішення.

```
S1(config)# interface range FastEthernet 0/1 - 2
S1(config-if-range)# channel-group 1 mode active
Creating a port-channel interface Port-channel 1
S1(config-if-range)# exit
S1(config-if)# interface port-channel 1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk allowed vlan 1,2,20
```

Рисунок 3.37 – Налаштування EtherChannel з LACP

Команда **show interfaces port-channel** відображає загальний стан інтерфейсу канального порту (рисунок 3.38).

```
S1# show interfaces port-channel 1
Port-channel1 is up, line protocol is up (connected)
  Hardware is EtherChannel, address is c07b.bcc4.a981 (bia c07b.bcc4.a981)
  MTU 1500 bytes, BW 200000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
(output omitted)
```

Рисунок 3.38 – Використання команди **show interfaces port-channel**

Якщо на одному пристрої налаштовано кілька інтерфейсів канальних портів, можна використовувати команду **show etherchannel summary** для відображення короткої інформації для кожного канального порту. На рисунку 3.39 показано, що в комутаторі налаштований один канал EtherChannel, номер групи 1, група використовує LACP. Канальна група складається з інтерфейсів FastEthernet0 / 1 і FastEthernet0 / 2. Група є каналом EtherChannel 2-го рівня, що відзначено буквами SU поруч з номером каналу порту.

```
S1# show etherchannel summary
Flags:  D - down        P - bundled in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      N - not in use, no aggregation
        f - failed to allocate aggregator
        M - not in use, minimum links not met
        m - not in use, port not aggregated due to minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port
        A - formed by Auto LAG
Number of channel-groups in use: 1
Number of aggregators:           1
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1      Po1(SU)         LACP      Fa0/1(P)    Fa0/2(P)
```

Рисунок 3.39 – Використання команди **show etherchannel summary**

Команда **show etherchannel port-channel** відображає інформацію про певний інтерфейсі канального порту (рисунок 3.40). У прикладі на рис. 15 інтерфейс Port Channel 1 складається з двох фізичних інтерфейсів, FastEthernet0 / 1 і FastEthernet0 / 2. Він використовує LACP в активному режимі. Він належним чином підключений до іншого комутатора з сумісною конфігурацією, тому показано, що канал порту використовується.

```
S1# show etherchannel port-channel
                Channel-group listing:
                ----------------------

Group: 1
----------
                Port-channels in the group:
                ---------------------------
Port-channel: Po1    (Primary Aggregator)
------------
Age of the Port-channel   = 0d:01h:02m:10s
Logical slot/port   = 2/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP
Port security       = Disabled
Load share deferral = Disabled
Ports in the Port-channel:
Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Fa0/1    Active             0
  0     00     Fa0/2    Active             0
Time since last port bundled:    0d:00h:09m:30s    Fa0/2
```

Рисунок 3.40 – Використання команди **show etherchannel port-channel**

На будь-якому фізичному елементі інтерфейсу канальної групи EtherChannel команда **show interfaces etherchannel** може надати інформацію про роль даного інтерфейсу в EtherChannel. Рисунок 3.41 показує, що інтерфейс FastEthernet0 / 1 є частиною канальної групи EtherChannel 1. Протоколом для цього EtherChannel є LACP.

```
S1# show interfaces f0/1 etherchannel
Port state    = Up Mstr Assoc In-Bndl
Channel group = 1           Mode = Active          Gcchange = -
Port-channel  = Po1         GC   =   -             Pseudo port-channel = Po1
Port index    = 0           Load = 0x00            Protocol =   LACP
Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDUs.
        A - Device is in active mode.        P - Device is in passive mode.
Local information:
                          LACP port     Admin     Oper    Port
Port      Flags   State     Priority      Key       Number  State
Fa0/1     SA      bndl      32768         0x1       0x1     0x102       0x3D
Partner's information:
                LACP port                       Admin  Oper   Port    Port
Port      Flags   Priority  Dev ID          Age   key    Key    Number  State
Fa0/1     SA      32768     c025.5cd7.ef00  12s   0x0    0x1    0x102   0x3Dof the port in the
current state: 0d:00h:11m:51sllowed vlan 1,2,20
```

Рисунок 3.41 – Використання команди **show interfaces etherchannel**

Поширені проблеми з конфігураціями EtherChannel

Всі інтерфейси в EtherChannel повинні мати однакову конфігурацію швидкості і дуплексного режиму, native і дозволені VLAN на з'єднувальних лініях і доступ до VLAN на портах доступу. Забезпечення цих змін значно зменшить можливі проблеми мережі, пов'язані з EtherChannel.

Поширені помилки EtherChannel можуть включать в себе наступні:

1. Призначені порти в EtherChannel не є частиною однієї VLAN або не налаштовані як транки.
2. Порти з різними native VLAN не можуть формувати EtherChannel.
3. Транкінг був налаштований на деяких портах, що складають EtherChannel, але не на всіх.
4. Якщо допустимий діапазон VLAN не збігається, порти не формують EtherChannel, навіть якщо PAgP встановлений в автоматичний або бажаний режим.
5. Параметри динамічного узгодження для PAgP і LACP не сумісні на різних кінцях EtherChannel.

Примітка: легко сплутати PAgP або LACP з DTP, оскільки всі вони є протоколами, що використовуються для автоматизації поведінки на магістральних каналах. PAgP і LACP використовуються для агрегації каналів (EtherChannel). DTP використовується для автоматизації створення магістральних посилань. Коли налаштована магістральна лінія EtherChannel, зазвичай спочатку налаштовується EtherChannel (PAgP або LACP), а потім DTP.

Крім об'єднання фізичних каналів в один логічний канал, Etherchannel забезпечує також Load-Balance – «балансування» (розподіл) завантаження, що надходить на передачу логічного каналу, між окремими фізичними каналами з його складу. Режим роботи Load-Balance перевіряється командою **show etherchannel load-balance** (рисунок 3.42).

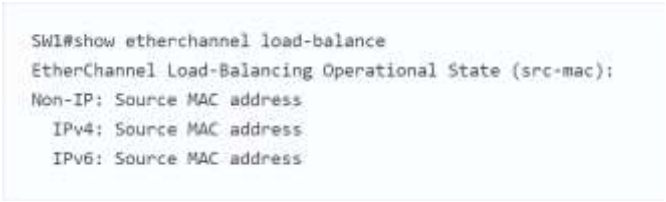


Рисунок 3.42 – Перевірка режиму роботи Load-Balance за допомогою команди **show etherchannel load-balance**

В даному прикладі LACP виконує балансування виходячи із значення MAC-адреси джерела, тобто кадри від 1-ого MAC-адреси будуть передані через першу лінію, від 2-ого MAC-адреси через другу лінію, від 3-ого MAC-адреси знову через першу лінію і так буде чергуватися. Але такий підхід не завжди вірний. Наприклад, є якась умовна мережу (рисунок 3.43), в ній SW1 підключені 2 комп'ютери, далі цей комутатор з'єднується з SW2 агрегованих

каналом, а до SW2 поключается маршрутизатор. За замовчуванням Load-Balance налаштований на значення MAC-адреси джерела. В результаті з боку SW1 кадри з MAC-адресою 111 будуть передаватися по першій лінії, а з MAC-адресою 222 по другій лінії. З боку SW2 є тільки підключення одного маршрутизатора з MAC-адресою 333, і всі кадри від маршрутизатора будуть відправлятися на SW1 по першій лінії. Відповідно, друга лінія буде завжди простоювати. Тому логічніше тут налаштувати балансування не по Source MAC-адресу, а по Destination MAC-адресу. Тоді все, що відправляється 1-го комп'ютера, буде відправлятися по першій лінії, а другого - по другій лінії.

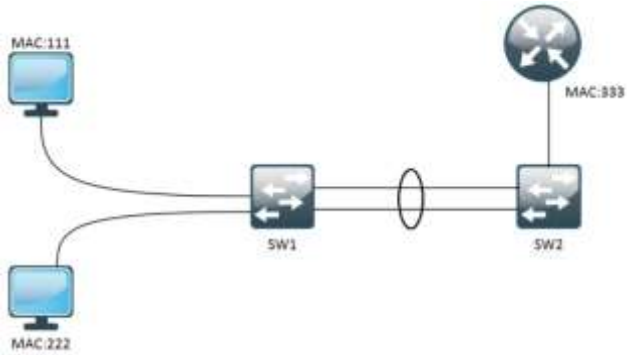


Рисунок 3.43 – Приклад мережі

Зміна режиму балансування виконується командою (рисунок 3.44) – **portchannel load-balance [argument].**

```
SW1(config)#port-channel load-balance ?
dst-ip Dst IP Addr
dst-mac Dst Mac Addr
src-dst-ip Src XOR Dst IP Addr
src-dst-mac Src XOR Dst Mac Addr
src-ip Src IP Addr
src-mac Src Mac Addr
```

Рисунок 3.44 – Зміна режиму балансування за допомогою команди **portchannel load-balance [argument]**

ЛЕКЦІЯ 4
ВИДИ, ПОБУДОВА і ПРИЗНАЧЕННЯ МОДЕМІВ

4.1. Призначення і загальні відомості про модеми

Нагадаємо, що систему передачі даних можна представить у вигляді моделі, що представлена на рисунку 3.45 (тема 1, лекція 1).

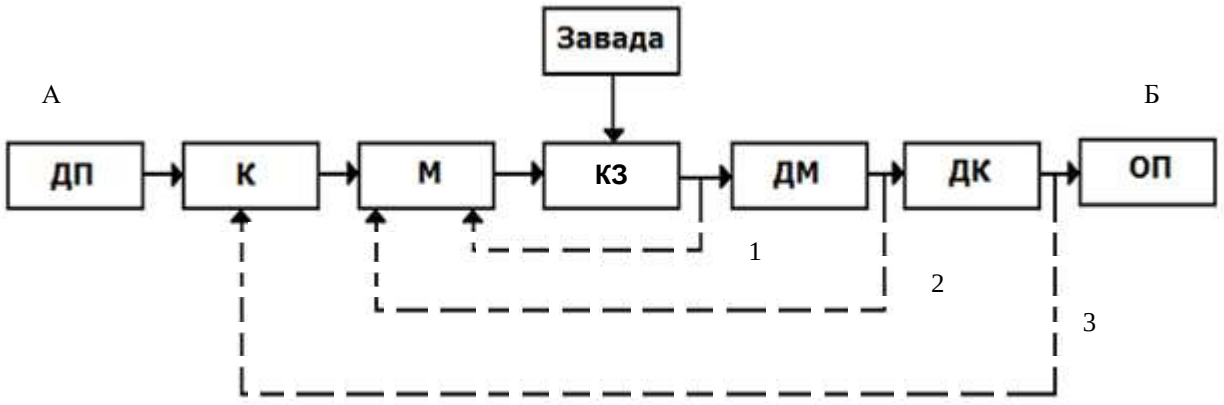


Рисунок 3.45 – Модель системи передачі даних

де, ДП – джерело повідомлення; К – кодер; М – модулятор; КЗ – канал електрозв'язку; ДМ – демодулятор; ДК – декодер; ОП – одержувач повідомлення.

Питання, які розглядалися в темі 2, відносилися до принципів побудови кодерів (К) і декодерів (ДК), що забезпечують завадостійке кодування сигналів передачі даних, а в темі 4 – побудови джерел і одержувачів повідомлень.

Предметом даної теми є принципи побудови модуляторів (М) та демодуляторів (ДМ), які при конструктивному з'єднанні в одному пристрої називають ***модемами***, до функцій яких належить в першу чергу збільшення відстані передачі сигналів даних, для чого вони забезпечують перетворення цих сигналів до вигляду найбільш адаптованого для передачі у каналі зв'язку визначеного типу із зворотнім перетворенням на прийомі), а в деяких випадках і утворюють канал зв'язку.

Фактично модем виконує функції лінійної частини апаратури передачі даних (АПД), що згідно міжнародних стандартів позначається як DCE (Data Communications Equipment) та забезпечує передавання даних між двома і більшою кількістю кінцевих терміналів по каналу визначеного типу (наприклад, по телефонному каналу).

Функції сучасних модемів належать до двох рівнів:

- фізичного;
- канального.

Фізичний рівень

Даний рівень визначає інтерфейси модему з каналом зв'язку, а саме, механічні, електричні, функціональні та процедурні параметри з'єднання.

На фізичному рівні виконуються три основні функції:

1) Встановлення і роз'єднання з'єднань взаємодіючих систем (фізичне підключення, узгодження способу модуляції, швидкості передачі, режимів виправлення помилок і стиснення даних).

2) Перетворення сигналів з метою узгодження параметрів інформаційного сигналу, що передається, з параметрами каналу.

Функція перетворення сигналів є головною функцією модемів. Тому модеми, які не мали інтелектуальних можливостей і не виконували апаратне стиснення і корекцію помилок, називали пристроями перетворення сигналів (ППС).

3) Реалізація інтерфейсу.

Інтерфейси між DTE і DCE регламентуються відповідними рекомендаціями і стандартами: V.24, RS-232, RS-449, RS-422A, RS-423A, V.35 та ін., які **визначають такі характеристики:**

– загальні (швидкість і послідовність передачі);

– функціональні та процедурні (номенклатура, категорія ланцюгів інтерфейсу, правила їх взаємодії);

– електричні (величини напруг, струмів і опорів);

– механічні (габарити, розподіл контактів).

Канальний рівень

На канальному (другому) рівні реалізуються такі основні функції:

– формування з послідовності біт інформаційних кадрів для передачі по каналу;

– кодування кадру завадостійким кодом (з виявленням помилок);

– відновлення початкової послідовності даних на приймальній стороні;

– забезпечення кодонезалежної передачі даних (припускає довільний вибір коду подання даних);

– управління потоком даних на рівні каналу, тобто швидкість їх видачі в DTE одержувача;

– усунення наслідків втрат, спотворень або дублювання кадрів, що передаються в каналі.

Як стандарт для протоколів другого рівня організацією ISO рекомендується протокол HDLC (High Level Data Link Control) та його спрощені версії для конкретної області застосування:

LAPB (Link Access Procedure Balanced), LAPD (Link Access Procedure D-channel) для застосовання в цифрових мережах ISDN, LAPM (Link Access Procedure for Modems) – базовий для стандарту корекції помилок V.42, LAPX (Link Access Procedure Extention) є напівдуплексним варіантом HDLC і

використовується в термінальних мережах і системах, працюючих в стандарті Teletex, а протокол LLC (Link Logic Control) реалізований практично у всіх мережах з множинним доступом.

4.2. Класифікація модемів і типова структурна схема модема

Класифікація модемів

Строгої класифікації модемів не існує й, імовірно, не може існувати через велику різноманітність як самих модемів, так і сфер застосування й режимів їх роботи. Проте можна виділити ряд ознак, по яких і провести умовну класифікацію. **До таких ознак або критеріїв класифікації можна віднести наступні:**

- область застосування;
- функціональне призначення;
- тип використовуваного каналу;
- конструктивне виконання;
- підтримка протоколів модуляції, виправлення помилок і стиску даних.

Можна виділити ще безліч більш детальних технічних ознак, таких як застосовуваний спосіб модуляції, інтерфейс сполучення з DTE і так далі.

За областю застосування розрізняють модеми для:

– телефонних каналів, що комутуються (модеми повинні вміти працювати з автоматичними телефонними станціями (АТС), розрізняти їхні сигнали й передавати свої сигнали набору номера);

– виділених каналів ТЧ (смуга пропускання обмежена значенням 3,1 кГц);

– фізичних (екранована й неекранована кручена пари, коаксіальний кабель, оптичне волокно і ін.) сполучних ліній:

- модеми низького рівня (лінійні драйвери) або модеми на короткі відстані (short range modems) (використовують цифрові сигнали),
- модеми основної смуги (baseband modems) (застосовують методи модуляції);

– цифрових систем передачі (CSU/DSU) (забезпечують підключення до стандартних цифрових каналів, таким як E1/T1 або ISDN, і підтримують функції відповідних канальних інтерфейсів);

– стільникових систем зв'язку (дозволяють передавати дані в умовах стільникових каналів з високим рівнем перешкод і постійно мінливими параметрами);

– для пакетних та локальних радіомереж (для передачі даних по радіоканалу між мобільними користувачами);

– і ін.

За методом передачі розрізняють:

– *асинхронні модеми* – які використовуються коли дані генеруються у випадкові моменти часу, наприклад користувачем. При такій передачі

обладнання повинне відновлювати синхронізацію на початку кожного одержуваного символу, що потребує додаткових стартових та стопових бітів для кожного переданого символу.

– *синхронні модеми* – якщо передані дані утворюють безперервну послідовність символів або байтів, то тактові генератори відправника й одержувача повинні бути синхронізовані протягом тривалого проміжку часу. У цьому випадку використовується синхронна передача.

В деяких випадках модем може працювати з комп'ютером в асинхронному режимі й одночасно з вилученим модемом – у синхронному режимі або навпаки. У такому випадку визначають, що модем *синхронно-асинхронний*.

За конструкцією розрізняють модеми:

- зовнішні;
- внутрішні;
- портативні;
- групові (сукупність окремих модемів, об'єднаних у загальний блок).

За інтелектуальними можливостями розрізняють модеми:

– без системи керування;

– з підтримкою набору АТ-команд (можливість повного управління характеристиками модему й параметрами зв'язку);

– з підтримкою команд V. 25bis (з управлінням режимами встановлення з'єднання й автовиклику);

– з фірмовою системою команд;

– з підтримкою протоколів мережного керування SMNP *(Simple Manager Network Protocol),* що дозволяє адміністраторові управляти елементами мережі (включаючи модеми) з вилученого термінала.

За підтримкою протоколів

Модеми також можна класифікувати відповідно до реалізованих у них протоколами. З функціональної точки зору модемні протоколи можуть бути розділені на наступні групи (рисунок 3.46):

1. Протоколи, що визначають норми взаємодії модему з каналом зв'язку (V.2, V.25).
2. Протоколи, що регламентують з'єднання й алгоритми взаємодії модему й DTE (V.10, V.11, V.24, V.25, V.25bis, V.28).
3. Протоколи модуляції, що визначають основні характеристики модемів, призначених для телефонних каналів, що комутуються, й виділених. До них ставляться такі протоколи, як V.17, V.22, V.32, V.34, HST, Zyx і велика кількість інших.
4. Протоколи захисту від помилок (V.41, V.42, MNP1-MNP4).
5. Протоколи стиску переданих даних, такі як MNP5, MNP7, V.42bis.
6. Протоколи, що визначають процедури діагностики модемів, випробування й виміру параметрів каналів зв'язку (V.51, V.52, V.53, V.54, V.56).

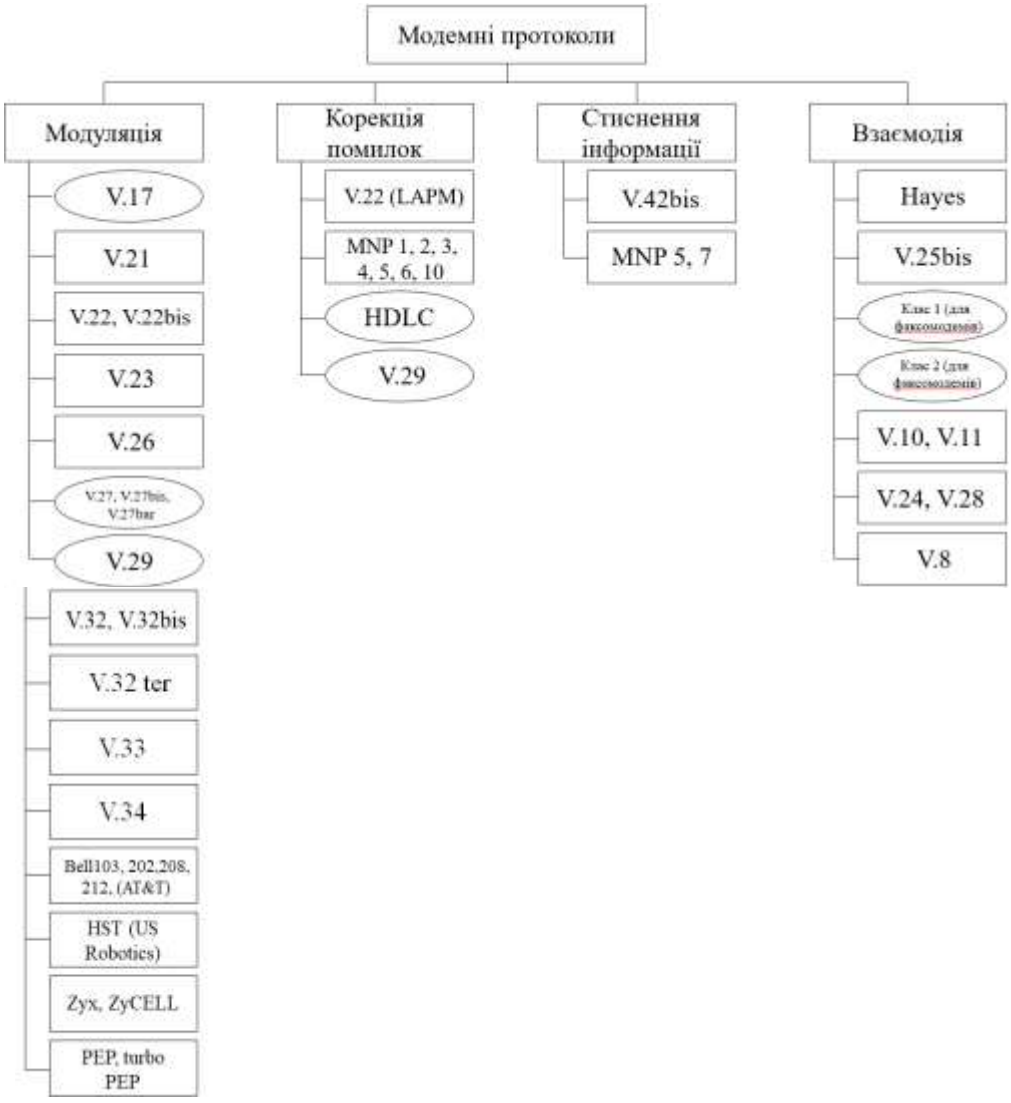


Рисунок 3.46 – Класифікація модемних протоколів

Типова структурна схема модема

Узагальнена структурна схема сучасного модема наведена на рисунку 3.47.

Модем має два адаптера портів – канального і DTE. Задача цих інтерфейсів погодження входу модема з каналом зв'язку і виходом обладнання передачі даних (інтерфейс DTE).

Якщо ж модем внутрішній, то замість інтерфейсів DTE може застосовуватися інтерфейс внутрішньої шини відповідного пристрою.

Порт канального інтерфейса забезпечує погодженість електричних параметрів з використовуємим каналом зв'язку. Канал може бути аналоговим або цифровим, з двох- або чотирьохпровідним закінченням.

Універсальний процесор (PU) – виконує функції управління взаємодією з DTE і схемами індикації стану модема. Саме він виконує АТ-команди посилаємі DTE і управляє режимами роботи модема. Крім того універсальний процесор (PU) може реалізовувати операції компресії/декомпресії передаваємих даних.

Універсальний сигнальний процесор вирішує завдання аналізу якості каналу зв'язку та визначення відповідного протоколу модуляції (кодування згортковим кодом, і т.і.). Але безпосередньо операцією модуляції/демодуляції управляє спеціалізований модемний процесор, а кодуванням – цифровий сигнальний процесор.

Разом всі чотири процесори утворюють схему управління модемом.

Рисунок 3.47 – Структурна схема модема

Програма управління для універсального процесора (PU) зберігається в ПЗП (ROM). Перепрограмуванням модема проводять модернізацію модема або апгрейд (upgrade). В сучасних модемах для полегшення модернізації замість мікросхем ROM можуть використовуватися мікросхеми флєш-пам'яті (Flash ROM).

Схема перепрограмуємого запомитовуючого пристрою (ППЗП) зберігає установки модема під час його виключення (зникнення живлення).

Оперативний запам'ятовуючий пристрій (ОЗП) використовується для тимчасового збереження даних і виконання проміжних обчислень як універсальним, так і цифровим сигнальним процесором.

На основі аналізу структурної схеми модему (рисунок 3.47) утворюється спрощена функціональна схема модему (рисунок 3.48).

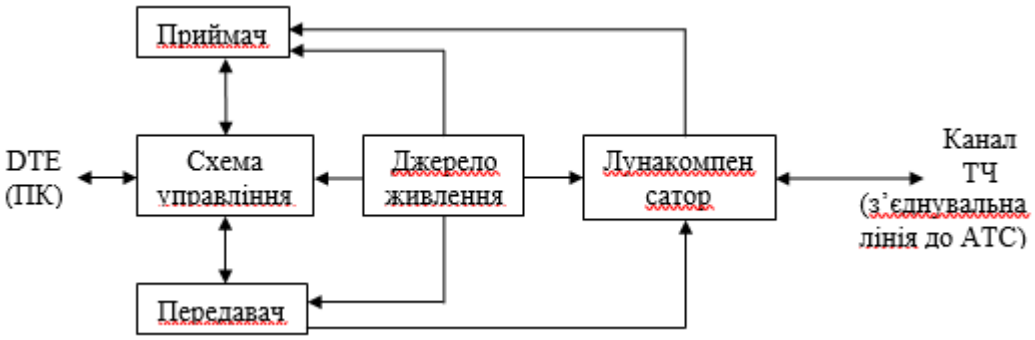


Рисунок 3.48 – Спрощена функціональна схема модему

Вона містить:

– схему управління (що об'єднує схеми та функції чотирьох процесорів, наведених на рис. 3);

– передавач (якій базується на частині обладнання порту канального інтерфейсу) – забезпечує модуляцію, кодування ЗСК та процедури підвищення достовірності передачі.

– приймач сигналів (якій також базується на частині обладнання порту канального інтерфейсу) – здійснює перетворення зворотні до передавача;

– компенсатор електричної луни – забезпечує одночасну роботу передавальної та приймальної частини модему в одному фізичному середовищі;

– джерело живлення, що забезпечує утворення градацій напруги необхідних для роботи всіх модулів модему.

Основні функції приймача і передавача виконуються цифровим сигнальним процесором (DSP) і модемним процесором.

Функціональна схема передавача модема наведена на рисунку 3.49.

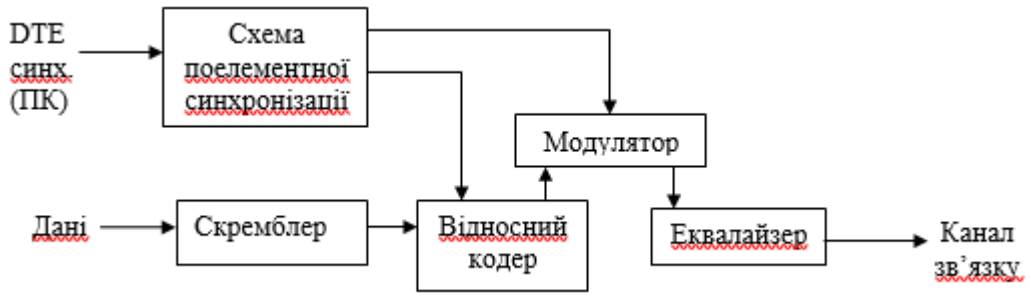


Рисунок 3.49 – Передавач модема

Схема поелементної синхронізації – отримує сигнал синхронізації через 24 контакт (DB-25) інтерфейсу RS-232 від обладнання передачі даних і забезпечує синхрону роботу модему з DTE.

Скремблер – перемішує символи даних з метою покращення роботи системи поелементної синхронізації приймача.

Модулятор у парі з **відносним кодером** реалізують прийнятий вид модуляції (формують модуляційний сигнал КАМ, АФМ, багатомірну КАМ, багатопозиційний сигнал).

Еквалайзер – вносить передпошкодження, що компенсує можливі викривлення в каналі.

Функціональна схема приймача наведена на рисунок 3.50.

Адаптивний еквалайзер компенсує нелінійні пошкодження сигналів, що вносятся каналом.

Демодулятор з **відносним декодером** – демодулюють модульований (АФМ, КАМ і т.і.) сигнал і видають на дескремблер послідовність символів.

Дескремблер відновляє порядок слідування розрядів даних і видає їх на термінал (ПК).

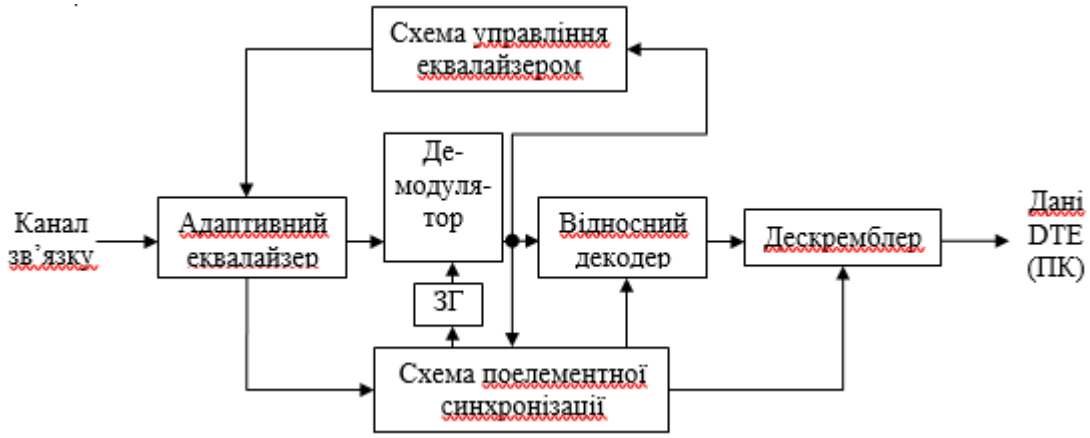


Рисунок 3.50 – Функціональна схема приймача

Схема поелементної синхронізації реалізує задачі по підтримці синхронізму приймача під передавача.

4.3. Варіанти застосування модемів

Для підключення за межами локальної мережі потрібно глобальна мережа (WAN). WAN - це телекомунікаційна мережа, яка охоплює більшу географічну зону, набагато більше географічного охоплення локальної мережі. Фізична топологія, яка в WAN, складна і здебільшого невідома користувачам. Замість цього топології WAN описуються з використанням логічної топології. Логічні топології описують віртуальне з'єднання між джерелом і призначенням.

Фізично користувач знає тільки найближчий до нього сегмент WAN, тому з'єднання споживача (тобто компанії / клієнта) або оператора зв'язку WAN представляють, як показано на рисунку 3.51.

На рис. 7 використані наступні терміни (таблиця 3.2):

Таблиця 3.2 – Термінологія обладнання WAN-мереж

Термін WAN	Опис
Термінальне обладнання (DTE)	Це пристрій, який з'єднує абонентські локальні мережі з пристроєм зв'язку WAN (тобто DCE). Внутрішні хости відправляють свій трафік на пристрій DTE. DTE підключається до абонентської лінії через DCE. Пристрій DTE зазвичай є маршрутизатором, але може бути хостом або сервером.
Обладнання для передачі даних (DCE)	Також зване кінцеве обладнання передачі даних, це пристрій, що використовується для зв'язку з постачальником. DCE в першу чергу надає інтерфейс для підключення абонентів до каналу зв'язку в хмарі WAN.

Продовження таблиці 3.2

Обладнання для приміщення клієнта (CPE)	Це пристрої DTE і DCE (тобто маршрутизатор, модем, оптичний перетворювач), розташовані в межах підприємства.
Демаркаційна точка	Це фізичне місце розташування в будівлі або комплексі, яке офіційно відокремлює CPE від обладнання постачальника послуг. Точкою розмежування зазвичай є розподільна коробка для кабелів, розташована в приміщенні клієнта, яка з'єднує проводку CPE з абонентською лінією. Він визначає місце, де відповідальність за роботу мережі змінюється з абонента на постачальника послуг.
Абонентська лінія (або остання миля)	Це фізичний мідний або оптоволоконний кабель, який з'єднує CPE з CO постачальника послуг.
Центральний офіс (CO)	Це засіб або будівля локального постачальника послуг, яке з'єднує CPE з мережею постачальника.
Мережа	Це включає в себе транзитні, магістральні, повністю цифрові, волоконно-оптичні лінії зв'язку, комутатори, маршрутизатори та інше обладнання в мережі провайдера WAN.

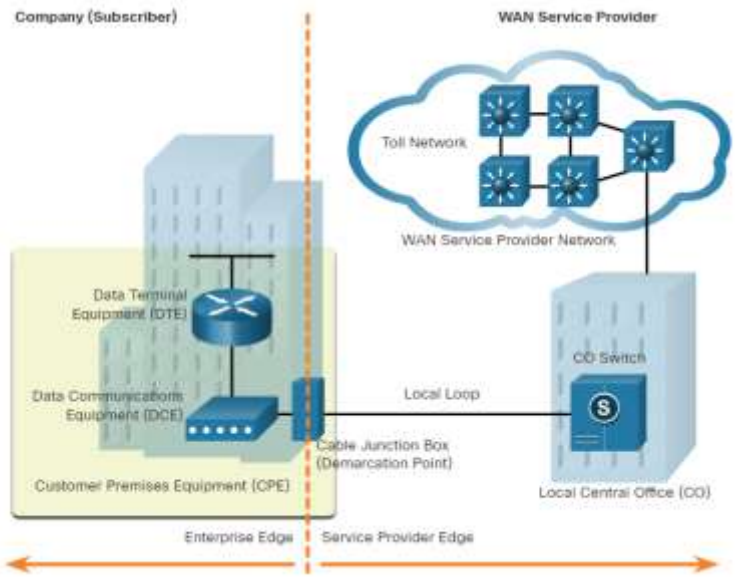


Рисунок 3.51 – З'єднання споживача (тобто компанії / клієнта) або оператора зв'язку WAN

Таким чином наскрізний шлях передачі даних по глобальній мережі зазвичай проходить (рисунок 3.52) від вихідного DTE до DCE, потім до хмари WAN, потім до DCE і, нарешті, до DTE призначення.

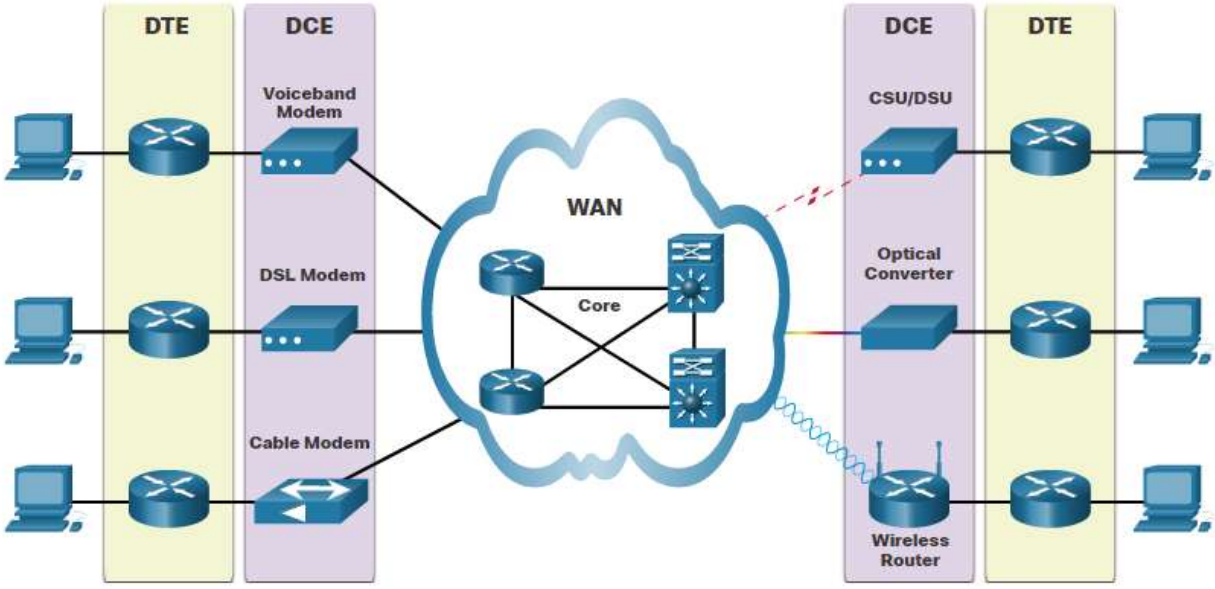


Рисунок 3.52 – Наскрізний шлях передачі даних по глобальній мережі

На рис. 8 використані наступні терміни (таблиця 3.3):

Таблиця 3.3

Пристрій WAN	Опис
Голосовий модем Voiceband	Модем комутованого доступу. Застаріле пристрій, що перетворював (тобто модулювати) цифрові сигнали, створювані комп'ютером, в аналогові мовні частоти. Використовує телефонні лінії для передачі даних.
DSL модем і кабельний модем	Це високошвидкісні цифрові модеми, відомі як широкосмугові модеми, підключаються до маршрутизатора DTE через Ethernet. DSL модеми підключаються до глобальної мережі за допомогою телефонних ліній. Кабельні модеми підключаються до глобальної мережі з використанням коаксіальних ліній. Обидва працюють аналогічно модему голосового діапазону, але використовують більш високі частоти широкосмугового доступу і швидкості передачі.
CSU/DSU	Для підключення цифрових ліній потрібні ЦСП (CSU / DSU). Вона підключає цифровий пристрій до цифрової лінії. CSU / DSU може бути окремим пристроєм, наприклад модемом, або інтерфейсом маршрутизатора. CSU забезпечує завершення лінійного тракту і забезпечує цілісність з'єднання за допомогою виправлення помилок і контролю лінії. DSU перетворює лінійні кадри в кадри, доступні LAN, і навпаки.

Продовження таблиці 3.3

Оптичний перетворювач	Також відомий як конвертер оптичного сигналу. Ці пристрої з'єднують оптоволоконні середовища з мідними і перетворять оптичні сигнали в електричні імпульси.
Безпровідний маршрутизатор або точка доступу	Пристрої використовуються для бездротового підключення до провайдера WAN. Маршрутизатор також можуть використовувати стільниковий бездротовий зв'язок.
Пристрій WAN Core	Магістраль WAN складається з декількох високошвидкісних маршрутизаторів і комутаторів рівня 3.

В результаті злиття користувачів мережі можна розділити на дротяні і бездротові. У **проводових варіантах** використовується постійна кабельна розводка (наприклад, мідна або оптоволоконний), що забезпечує постійну смугу пропускання, мале число помилок і затримку. Прикладами дротових широкосмугових з'єднань є цифрова абонентська лінія (DSL), кабельні з'єднання і оптоволоконні мережі.

Варіанти бездротового зв'язку дешевше в реалізації в порівнянні з іншими варіантами підключення до глобальної мережі, оскільки для передачі даних вони використовують радіохвилі замість дротових середовищ. Однак на бездротові сигнали можуть мати негативний вплив такі чинники, як відстань від радіовишек, перешкоди від інших джерел, погода і кількість користувачів, які отримують доступ до спільного простору. Приклади бездротового широкосмугового зв'язку включають в себе послуги стільникового зв'язку 3G / 4G / 5G або супутникового інтернету.

Модеми застосовуються для дротових варіантів, тому розглянемо далі їх.

Технологія DSL

Цифрова абонентська лінія (DSL) – це високошвидкісна, постійно включена технологія з'єднання, яка використовує існуючі телефонні лінії з кручений парою для надання користувачам послуг IP. На рисунку 3.53 показано розподіл смуги пропускання на мідному дроті для асиметричної DSL (ADSL).

Діапазон, позначений POTS, містить частотний діапазон, який використовується телефонної службою (ТМЗК). Діапазон, позначений ADSL, являє частотне простір, що використовується висхідними і спадними сигналами DSL.

Існує кілька різновидів xDSL, що пропонують різні швидкості передачі. Однак всі форми DSL підрозділяються на асиметричні DSL (ADSL) або симетричні DSL (SDSL). ADSL і ADSL2 + забезпечують більш високу пропускну здатність низхідного потоку для користувача, ніж завантажується

пропускна здатність. SDSL забезпечує однакову пропускну здатність в обох напрямках.

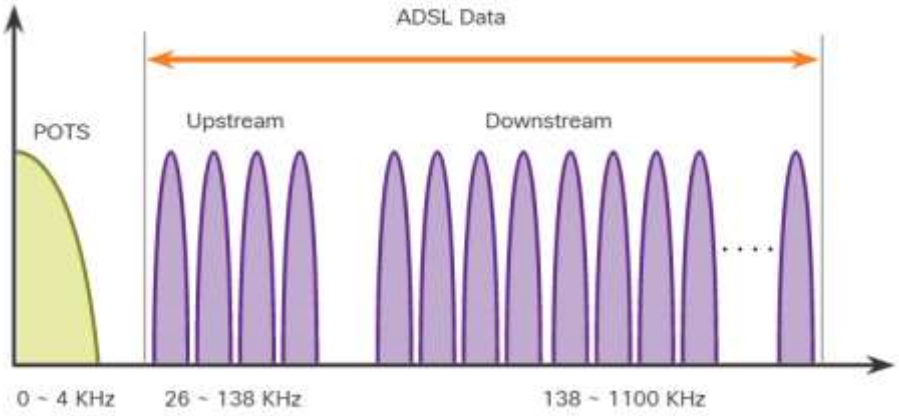


Рисунок 3.53 – Розподіл смуги пропускання на мідному дроті для асиметричної DSL (ADSL)

Швидкість передачі також залежить від фактичної довжини локальної петлі, а також від типу і стану кабелю. Наприклад, петля ADSL повинна бути менше 5,46 км (3,39 милі) для гарантованої якості сигналу.

DSL Connections

Постачальники послуг розгортають DSL-з'єднання в абонентської лінії. Як показано на рисунку 3.54, з'єднання встановлюється між модемом DSL і мультиплексором доступу DSL (DSLAM).

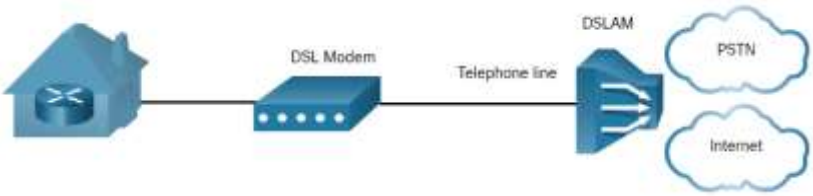


Рисунок 3.54 – Встановлення з’єднання між модемом DSL і мультиплексором доступу DSL (DSLAM)

На схемі показаний домашній маршрутизатор, підключений до модему DSL, який підключається по телефонній лінії до DSLAM і Інтернету.

Модем DSL перетворює сигнали Ethernet від віддаленого пристрою в сигнал DSL, який передається на мультиплексор доступу DSL (DSLAM) в місці розташування постачальника.

DSLAM – це пристрій, розташоване в центральному офісі (CO) провайдера, яке концентрує з'єднання від декількох абонентів DSL.

Перевага DSL перед кабельної технологією полягає в тому, що DSL не є загальним середовищем. Кожен користувач має окреме пряме з'єднання з DSLAM. Додавання користувачів не знижує продуктивність, якщо інтернет-

з'єднання DSLAM з Інтернет-провайдером або Інтернетом не стане насиченим.

DSL зазвичай використовується постачальниками телефонних послуг спільно з протоколом «точка-точка» (PPP) - це протокол рівня 2, що забезпечує встановлення з'єднань між маршрутизаторами, а також між хостом і мережею з комутацією каналів, і мереж доступу ISDN. **Він забезпечує:**

- аутентифікацію абонента;
- призначення абоненту публічного IPv4-адреси;
- функції управління якістю зв'язку.

Модем DSL має інтерфейс DSL для підключення до мережі DSL і інтерфейс Ethernet для підключення до клієнтського пристрою. Однак Ethernet-канали з самого початку не підтримують PPP. Тому маршрутизатор налаштовується як клієнт PPPoE, як показано на рисунку 3.55. Маршрутизатор є клієнтом PPPoE і отримує свою конфігурацію від провайдера. Клієнти зв'язуються з маршрутизатором, використовуючи тільки Ethernet, і не знають про з'єднання DSL. У цій топології кілька клієнтів можуть спільно використовувати з'єднання DSL.

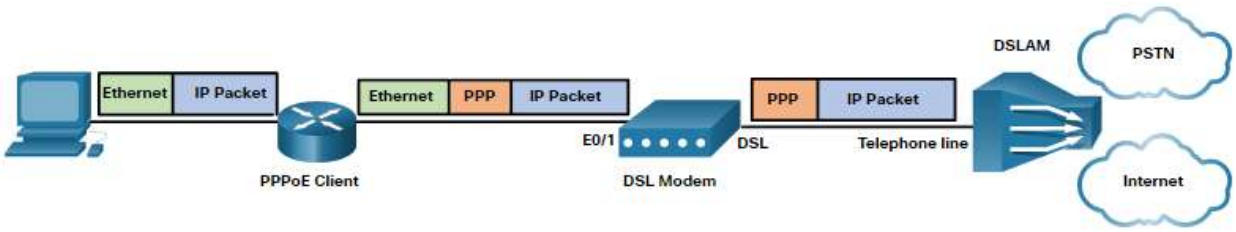


Рисунок 3.55 – Налаштування маршрутизатора як клієнта PPPoE

Кабельні модеми

Кабельна технологія – це високошвидкісна технологія постійного підключення, яка використовує коаксіальний кабель від кабельної компанії для надання IP-послуг користувачам. Сучасні кабельні системи в використанням специфікації DOCSIS пропонують клієнтам одночасний високошвидкісний доступ в Інтернет, цифрове кабельне телебачення і телефонний зв'язок.

Кабельні оператори часто розгортають гібридні волоконно-коаксіальні (HFC) мережі для забезпечення високошвидкісної передачі даних на кабельні модеми. HFC використовує оптоволоконний і коаксіальний кабель в різних частинах мережі. Наприклад, з'єднання між кабельним модемом і оптичним вузлом є коаксіальним кабелем, як показано на рисунку 3.56.

Оптичний вузол виконує перетворення оптичного сигналу в РЧ. Зокрема, він перетворює радіочастотні сигнали в світлові імпульси по оптоволоконному кабелю. Волоконно-оптичне середовище дозволяє сигналам проходити на великі відстані до головної станції постачальника, де розташована система завершення кабельного модему (CMTS). Головна

станція містить ресурси, необхідні для забезпечення доступу в Інтернет, в той час як CMTS відповідає за зв'язок з кабельними модемами.

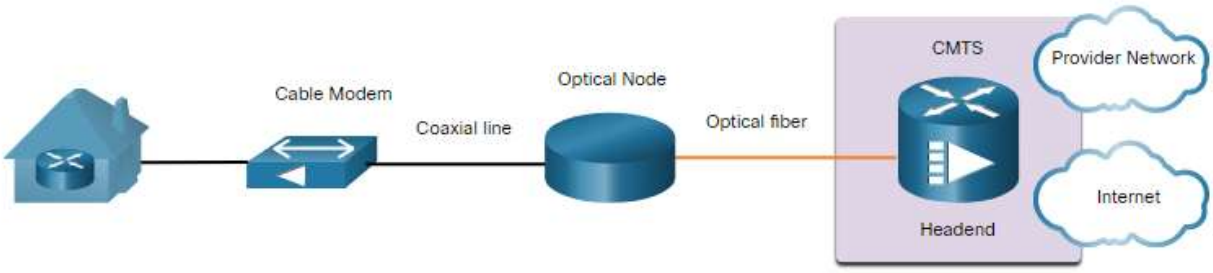


Рисунок 3.56 – З'єднання за допомогою коаксіального кабеля між кабельним модемом і оптичним вузлом

Оптоволокно

Багато операторів прокладають оптоволоконний кабель до місця знаходження користувача. Це зазвичай називають як Fiber to the x (FTTx) і включає в себе кілька різновидів:

Волокно до будинку (FTTH) – волокно досягає межі резиденції, кабельне телебачення, інтернет і телефонні послуги надаються користувачеві FTTH безпосередньо з центрального офісу постачальника послуг.

Волокно до будівлі (FTTB) – волокно досягає межі будівлі, наприклад, в підвалі багатоквартирного будинку, причому остаточне з'єднання з індивідуальним житловим простором здійснюється за допомогою альтернативних засобів.

Оптоволокно до вузла (FTTN) – оптичні кабелі досягають оптичного вузла, який перетворює оптичні сигнали в формат, прийнятний для кручений пари або коаксіального кабелю, що прокладається в приміщення.

FTTx може забезпечити найвищу пропускну здатність серед усіх варіантів широкосмугового доступу.

ЛЕКЦІЯ 5
ПРИНЦИПИ ПОБУДОВИ СИСТЕМИ ЕЛЕКТРОННОЇ ПОШТИ

5.1. Структура і функції системи електронної пошти

Системи транспортування повідомлень між людьми за допомогою комп'ютерних систем відомі під назвою електронної пошти. Системи електронної пошти є прикладним програмним забезпеченням і їх створення та функціонування регламентується стандартом МККТТ Х.400. Взагалі засоби електронної пошти можна віднести до систем обробки повідомлень (СОП).

Електронна пошта або **е-пошта** – спосіб обміну цифровими повідомленнями між людьми з використанням цифрових пристроїв, таких як комп'ютери та мобільні телефони, що робить можливим пересилання даних будь-якого змісту (текстові документи, аудіо-, відеофайли, архіви, програми).

Електронна пошта має справу з електронними повідомленнями, у вигляді файлів, підготовленими з допомогою комп'ютерної техніки, які обробляються і транспортуються теж засобами обчислювальної техніки та зв'язку. В класичних поштових системах, як ми знаємо, поштові відправлення транспортуються в матеріальній формі (листи, бандеролі, посилки) автомобільним, залізничним чи повітряним транспортом.

Тому можна визначити електронну пошту як службу поштового зв 'язку в якій доставка поштових повідомлень здійснюється електронними методами за допомогою комп 'ютерів.

Функціонування електронної пошти побудовано на принципі клієнт-сервер, стандартному для більшості мережевих сервісів. Кожний абонент, підключений до поштового серверу, має свою електронну адресу або, образно кажучи, поштову скриньку. Доступ до цієї поштової скриньки захищений паролем абонента. Абонент і сервер для обміну повідомленнями використовують кабель або звичайну телефонну лінію.

Носієм електронних повідомлень між поштовими серверами може бути мережа будь-якого масштабу. Повідомлення перед переходом з одного сервера на інший може проходити ряд проміжних серверів. Поштові сервери обмінюються повідомленнями в автоматичному режимі, при чому маршрут руху повідомлень в мережі вибирається маршрутизаторами. Коли повідомлення надходять на сервер призначення, адресат при черговому з’єднанні із сервером одержує повідомлення про надходження пошти. Повідомлення електронної пошти знаходить свого адресата за допомогою поштової адреси (E-mail). Ця адреса складається з двох частин, розділених значком @. Ліва частина адреси – це локальне ім’я користувача (ім’я поштової скриньки), а права частина – ім’я домену. Значок @ просто кажучи «собака», означає прийменник at («у, при»). Щоб користувач міг надсилати й одержувати електронні повідомлення, на його комп’ютері слід встановити програмне забезпечення клієнта електронної пошти. Існують різні поштові

програми, які мають різні можливості і призначені для роботи в різних операційних системах. Широко застосовуються поштові програми Microsoft Exchange, Outlook Express, Microsoft Outlook, Internet Mail, Eudora, Exchange Mail тощо. Часто ці програми включають до складу ОС.

Загальні функції системи електронної пошти:

– підготовка тексту;
– імпорт файлів-додатків;
– відправка листа;
– перегляд і збереження кореспонденції;
– знищення кореспонденції;
– підготовка відповіді;
– коментування і пересилка інформації;
– експорт файлів-додатків.

Електронна пошта має такі переваги і особливості:

– простота і дешевизна, відстань пересилання і країна доставки не мають значення;

– обсяг листів може бути досить великим (він обмежений лише пропускною спроможністю ліній передачі, а також простором на сервері, який надають ящику);

– доставка зазвичай відбувається дуже швидко (протягом декількох хвилин), негарантований час пересилки і відсутність інтерактивності;

– можливість пересилки нетекстової інформації;
– висока надійність доставки;

– потенційна можливість доступу для третіх осіб під час пересилки, при можливості підписати і зашифрувати лист.

На рисунку 3.57 показана типова послідовність подій, що відбуваються, коли абонент 1 відправляє електронного листа абоненту 2:

Рисунок 3.57 – Послідовність подій, що відбуваються, коли абонент 1 відправляє електронного листа абоненту 2

1. Абонент 1 за допомогою будь-якого редактора створює повідомлення.

2. За допомогою поштової програми **(MUA)** абонент 1 створює лист, вводить e-mail адресата і відправляє його за певним протоколом на місцевий сервер обміну пошти **(MTA)** поштового провайдера.

3. MTA – агент передачі повідомлень пересилає і розміщує їх в ящику одержувачів. Завдання транспортних агентів - приймати пошту від агента MUA і переправляти пошту на відповідні сервери (машини) для доставки, а також приймати пошту від інших транспортних агентів. Одержувачами повідомлень ЕП можуть бути, як користувачі однієї системи, так і віддалених систем. MTA відповідає також за маршрутизацію поштового повідомлення всіма доступними засобами для доставки його одержувачу. Якщо MTA не може знайти відповідний шлях для передачі повідомлення (листи) одержувачу, то він визначає сервер для пересилання повідомлення або ж повертає повідомлення відправнику з відміткою про неможливість доставки. Кожен агент MTA на шляху переміщення повідомлення бере на себе відповідальність за доставку повідомлення в кінцевий пункт призначення, а прі не можливості доставки він повертає лист його відправнику.

4. В результаті лист з'являється в в скринці абонента 2.

5. Абонент 2 натискає кнопку «отримати повідомлення» в поштовому клієнті, і отримує листи з сервера.

Отже, електронна пошта заснована на взаємодії двох програм. Одна з них сервер, інша – клієнт.

Поштовий сервер – програма, яка забезпечує роботу служби з боку Інтернет.

Поштовий клієнт – програма, встановлена на комп'ютері користувача і забезпечує взаємодію з поштовим сервером (Outlook Express, The Bat!, Eudora, Pegasus Mail).

Вони взаємодіють за певними правилами, заданим в протоколах.

Система обробки повідомлень має забезпечити виконання наступних завдань:

- транспортування поштової кореспонденції;
- передавання та прийом повідомлень;
- адресацію.

Однією з головних особливостей систем обробки повідомлень с асинхронна природа зв'язку між користувачами.

Саме вона забезпечує переваги:

– не потребує присутності учасників під час сеансу обміну інформацією. Особливо це може бути корисним у випадках різних часових поясів, коли зв'язок по телефону неможливий або незручний;

– з технічної точки зору побудована як мережа комутації повідомлень на всіх рівнях моделі, що забезпечує високий ступінь використання ресурсів, можливість перетворення форматів, кодів тощо;

– можливість ефективних двосторонніх і багатосторонніх зв'язків. Передача повідомлень, одночасно багатьом користувачам, забезпечується механізмом формування адреси на конверті або служби розподільних листів;

– СОП є одною з складових системи автоматизації фінансових установ, яка забезпечує обмін повідомленнями, що створюються, обробляються, передаються, приймаються та зберігаються з допомогою електронних систем.

Очевидно, що за таких умов СОП може взаємодіяти з різними обчислювальними мережами. Тому для з'єднання різних мереж необхідний шлюз.

Шлюз – це устаткування, що призначене для з'єднання двох мереж:, які є різними за адресацією, протоколами чи форматами даних. **Можна виділити наступні типи шлюзів:**

– **Протокольний шлюз** – призначений для з'єднання мереж передачі даних з різними протоколами шляхом перетворення сервісних елементів однієї мережі в сервісні елементи іншої.

– **Адресний шлюз** – об'єднує мережі з різними системами адресації.

– **Шлюз форматів** – забезпечує перетворення форматів різних стандартів систем електронної пошти (МККТТ X.400, UUCP) та первинних кодів (ASCII, EBDIC).

Визначимося з поняттям адресації в електронній пошті. Нехай ідентифікатор – однозначно визначає ресурс, який належить певному власнику чи системі, котра формується визначеним простором імен або ідентифікаторів. Адреса – визначає місце розташування ресурсу відносно системи адресації, яка формується визначеним адресним простором. Шлях – указує на те, як знайти ресурс. **Для цього використовуються наступні методи маршрутизації:**

- маршрутизація від джерела, коли відправник повідомлення не визначає весь шлях проходження повідомлення. В даному випадку він користується інформацією про структуру мережі і каналів зв'язку між вузлами;

- внутрішня маршрутизація, коли відправник не визначає маршрут доставки повідомлення одержувачу. В даному випадку діє система відображення маршруту для того, щоб в кожному транзитному вузлі автоматично визначався шлях до наступного вузла.

5.2. Характеристика протоколів електронної пошти

Протокол служби – технічний стандарт (система правил), який визначає технічні особливості взаємодії поштових серверів один з одного і з поштовими клієнтами.

Для роботи з електронною поштою **використовуються прикладні протоколи:**

– SMTP;

– POP3;

– IMAP4.

Протокол SMTP (Simple Massage Transfer Protocol) — простий протокол, що підтримує передачу повідомлень між будь-якими вузлами Інтернет. Маючи механізми проміжного збереження пошти і підвищення надійності доставки, протокол SMTP припускає використання різноманітних транспортних служб і поштових серверів. Він може працювати навіть в мережах, які не підтримують стек протоколів TCP/IP. Протокол SMTP дозволяє групувати повідомлення на адресу одного одержувача і розмножувати копії E-mail-повідомлення для передачі за різними адресами.

Він застосовується для передачі повідомлень по TCP-з'єднання від клієнта до сервера і між поштовими серверами MTA. Взаємодія в рамках SMTP будується за принципом двостороннього зв'язку, яка встановлюється між відправником і отримувачем поштового повідомлення. При цьому відправник ініціює з'єднання і посилає запити на обслуговування, а одержувач - відповідає на ці запити. Фактично відправник виступає в ролі клієнта, а в ролі одержувача - сервер (рисунок 3.58).

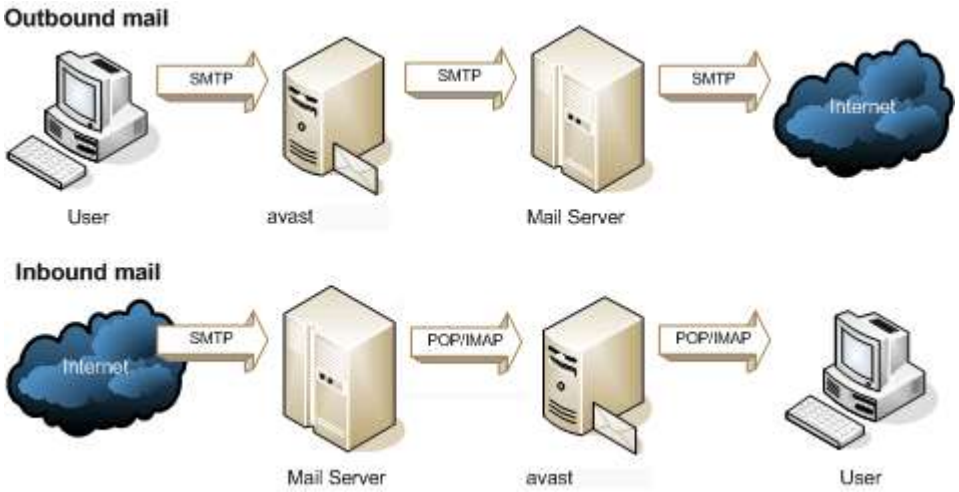


Рисунок 3.58 – Послідовність подій, де відправник виступає в ролі клієнта, а в ролі одержувача - сервер

Канал зв'язку встановлюється безпосередньо між відправником і отримувачем повідомлення. При такій взаємодії пошта сягає абонента протягом декількох секунд після відправлення.

Обмін командами і відповідями на них називається поштового транзакцією (mail transaction).

Перші системи електронної пошти використовували протокол UUCP (Unix-to-Unix Communication Protocol). Хоча більшість сучасних поштових серверів базуються на протоколі SMTP, протокол UUCP продовжує застосовуватися в багатьох додатках, які використовують ОС UNIX.

UUCP – протокол визначає взаємодію між двома поштовими програмами, встановленими в різних комп'ютерах. Цей діалог включає у себе

три етапи: встановлення каналу, послідовність запитів пересилки файлів і закриття каналу (рисунок 3.59).

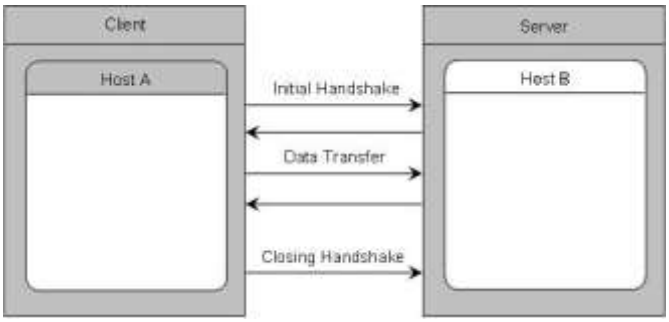


Рисунок 3.59 – Взаємодія між двома поштовими програмами, встановленими в різних комп'ютерах

Отже особливість протоколу полягає у відсутності поштових серверів. Ініціатора обміну називають клієнтом (в літературі можна також зустріти також назву master), а другий хост - сервером (slave). Отже розподіл функцій залежить від того, який комп'ютер відправляє першу команду, тобто в різних сеансах їх функції змінюються.

Протокол POP (Post Office Protocol, POP3) – протокол доставки пошти користувачеві з поштової скриньки поштового сервера POP. Багато концепції, принципи і поняття протоколу POP виглядають і функціонують подібно SMTP. Команди POP практично ідентичні командам SMTP, відрізняючись в деяких деталях. На рисунку 3.60 зображена модель клієнт-сервер по протоколу POP. Сервер POP знаходиться між агентом користувача і поштовими скриньками.

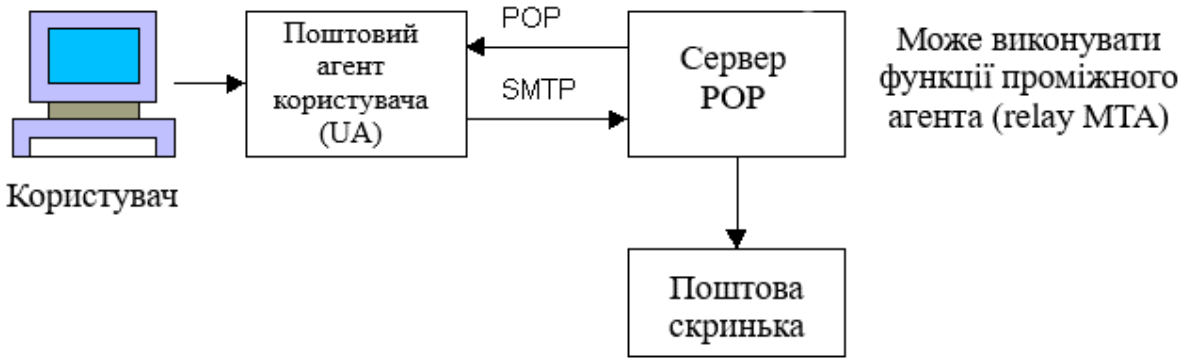


Рисунок 3.60 – Модель клієнт-сервер по протоколу POP

Конструкція протоколу POP3 забезпечує можливість користувачеві звернутися до свого поштового сервера і повністю вилучити пошту, яка накопичилася для нього. Користувач може отримати доступ до POP-серверу з будь-якої точки доступу до Інтернет. При цьому він повинен запустити спеціальний поштовий агент (UA), який працює по протоколу POP3, і налаштувати його для роботи зі своїм поштовим сервером. У протоколі POP3

обумовлені три стадії процесу отримання пошти: авторизація, транзакція і оновлення. Після того як сервер і клієнт POP3 встановили з'єднання, починається стадія авторизації. На стадії авторизації клієнт ідентифікує себе для сервера. Якщо авторизація пройшла успішно, сервер відкриває поштову скриньку клієнта і починається стадія транзакції. У ній клієнт або запитує у сервера інформацію (наприклад, список поштових повідомлень), або просить його зробити певну дію (наприклад, видати поштове повідомлення). Нарешті, на стадії оновлення сеанс зв'язку закінчується.

IMAP (англ. Internet Message Access Protocol – «Протокол доступу до інтернет-повідомленнями») – мережевий протокол прикладного рівня для доступу до електронної пошти.

Аналогічно POP3, щоб виконувати завдання із вхідними листами, проте забезпечує додаткові функції, зокрема, можливість пошуку за ключовим словом без збереження пошти в локальній пам'яті.

IMAP надає призначені для користувача великі можливості для роботи з поштовими скриньками, розташованими на центральному сервері. Поштовий клієнт, який використовує цей протокол, отримує доступ до сховища кореспонденції на сервер так, начебто ця кореспонденція розташована на комп'ютері одержувача. Електронними листами можна маніпулювати з комп'ютера користувача (клієнта) без постійної пересилання з сервера і назад файлів з повним змістом листів. Для відправлення листів використовується протокол SMTP.

IMAP був розроблений для заміни більш простого протоколу POP3 і має такі переваги в порівнянні з останнім:

Листи зберігаються на сервері, а не на машині клієнта. Можливий доступ до одного і того ж поштової скриньки з різних клієнтів. Підтримується також одночасний доступ декількох клієнтів. У протоколі є механізми, за допомогою яких клієнт може бути проінформований про зміни, зроблених іншими клієнтами.

Підтримка декількох поштових скриньок (або папок). Клієнт може створювати, вилучати і перейменовувати поштові скриньки на сервері, а також переміщати листи з однієї поштової скриньки в інші.

Можливе створення спільних папок, до яких можуть мати доступ декілька користувачів.

Інформація про стан листів зберігається на сервері і доступна всім клієнтам. Листи можуть бути позначені як прочитані, важливі і тому подібне

Підтримка пошуку на сервері. Немає необхідності завантажувати з сервера величезна кількість повідомлень для того, щоб знайти одне потрібно.

Підтримка онлайн-роботи. Клієнт може підтримувати з сервером постійне з'єднання, при цьому сервер в реальному часі інформує клієнта про зміни в поштових скриньках, в тому числі про нові листи.

Структура електронного листа

При передачі по протоколу SMTP електронного листа складається з наступних частин:

Даних SMTP-конверта

Ця інформація передається за межі сервера тільки в рамках протоколу SMTP, і зміна протоколу при доставці пошти (наприклад, на вузлі-одержувачі в процесі внутрішньої маршрутизації) може призводити до втрати цієї інформації. У більшості випадків ця інформація недоступна кінцевому адресату, який використовує не-SMTP протоколи (POP3, IMAP) для доступу до поштової скриньки. Для можливості контролювати працездатність системи ця інформація зазвичай зберігається в журналах поштових серверів. Містить:

– ім'я або рядок адреси вузла відправки;
– e-mail відправника;
– електронна адреса одного або декількох одержувачів.

Повідомлення (в термінології протоколу SMTP – 'DATA'), яке, в свою чергу, складається з двох частин, розділених символом нового рядка:

Тема (англ. Header) листи. У заголовку вказується службова інформація та позначки поштових серверів, через які пройшов лист, позначки про пріоритет, інформацію про те, схожий цей лист на спам, інформацію про перевірку антивірусами, рівень терміновості листи, вказівки на адресу та ім'я відправника і одержувача листа, тема листа і інша інформація.

Тіло (англ. Body) листи. У тілі листа міститься власне повідомлення листа.

5.3. Система адресації електронних повідомлень і можливості поштових клієнтів

Можливі дві системи адресації:

– явна адресація, історично притаманна UNIX-системам і названа UUCP (Unix-to-Unix Communication Protocol).

– доменна адресація DNS (Domain Name System), яка використовується в Internet.

При явній адресації маршрут до адресата вказується переліком імен комп'ютерів, через які послідовно передається лист (поштове повідомлення), файл з доповненням. Останнім ім'ям в цій послідовності є ім'я адресата (одержувача) на останньому зазначеному комп'ютері.

Наприклад, mail@odin.uucp: @ dept1.uucp: @ dept2: bill @ dept3

Ця команда відправляє пошту користувачеві bill @ dept3 через проміжні системи UUCP: odin і dept1, а потім - через проміжні системи локальної мережі dept2 і dept3.

При використанні доменної адресації адреса складається з двох частин: вхідного імені та імені домену. Ці дві частини розділяються знаком @: зліва від нього знаходиться вхідне ім'я, а справа – ім'я домену. Наприклад, адреса peterk@csn.org. Права частина peterk є вхідним ім'ям, а csn.org являє собою ім'я домену.

При пошуку імен в Internet використовується доменна система іменування (Domain Name System – DNS). Локальний сервер (комп'ютер) звертається перед усім до кореневого сервера, тобто комп'ютера, який знає номер, асоційований у вашому імені домену з доменом вищого рівня. Наприклад, для адреси peterk@csn.org. кореневий сервер повідомляє вашому локального сервера, який комп'ютер відповідає за домен .org. Після цього локальний сервер з'єднується з комп'ютером .org і питає, де знаходиться csn. Потім, маючи потрібний повний доменний номер, локальний сервер адресує повідомлення і відправляє його. Ім'я домену описує, де в мережі можна знайти наш комп'ютер. Це ми отримуємо при першому відкритті розрахунку. Internet відшукує ім'я домену, знаходить асоційований з ним номер (адреса комп'ютера, який працює в електронній мережі) і використовує номер для направлення повідомлення в потрібне місце.

Сучасний клієнт E-mail має добре організований інтерфейс (рисунок 3.61), що не вимагає багато часу і сил для засвоєння, і забезпечує наступні функції:

– приймати і відправляти пошту відразу з декількох поштових скриньок (адрес) (рисунок 3.62);

– створювати і відправляти повідомлення або повідомлення з вкладеннями одному одержувачу або відразу групі осіб (в тому числі приховані копії);

– сортувати і фільтрувати вхідні листи за встановленими правилами (рисунок 3.63);

– переадресовувати отриману пошту іншим особам;

– зберігати і вдосконалювати листи-чернетки, які ще не готові для відправки;

– створювати і використовувати шаблони для загального оформлення листів, а також для додавання в текст різної інформації службового характеру;

– читати / складати листи в автономному режимі;

– видаляти електронні листи;

– робити кілька підписів під створеним повідомленням;

– перевіряти орфографію;

– шифрувати повідомлення;

– реалізовувати засоби фільтрації або маршрутизації, тобто задавати правила, за якими програма повинна обробляти повідомлення;

– забезпечувати автоматичну відправку повідомлень і при відсутності користувача;

– створювати і застосовувати електронну адресну книгу з контактними адресами осіб або організацій

– зберігати і створювати як індивідуальні адреси e-mail, так і групові, тобто цілі списки розсилки;

– автоматично додавати до адресної книги e-mail адресу надходить повідомлення;

– автоматично здійснювати антивірусний контроль всієї поштової кореспонденції та доданих до неї файлів.

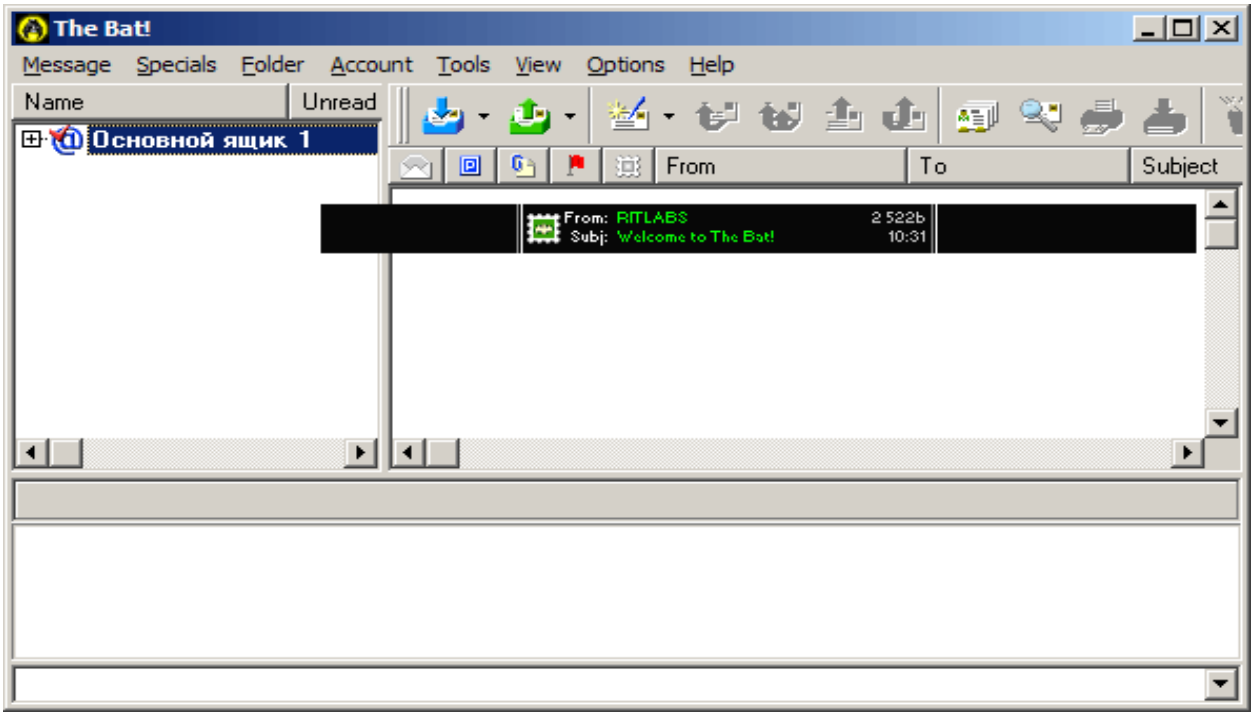
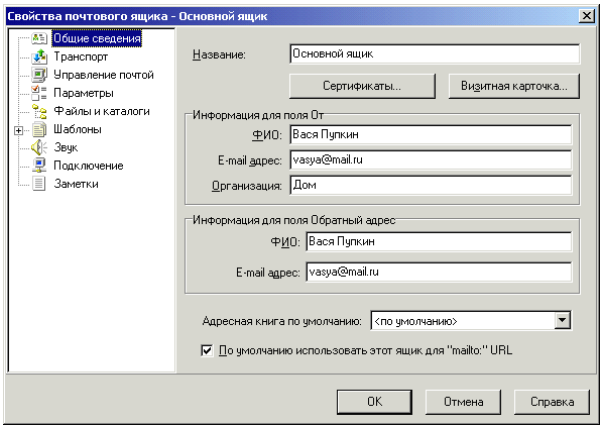


Рисунок 3.61 – Інтерфейс клієнта e-mail



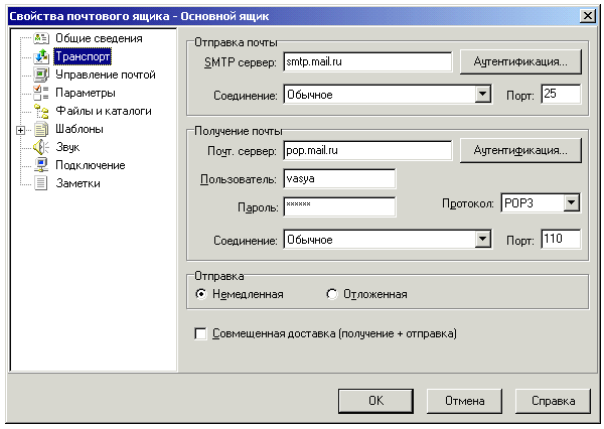


Рисунок 3.62 – Налаштування клієнта e-mail

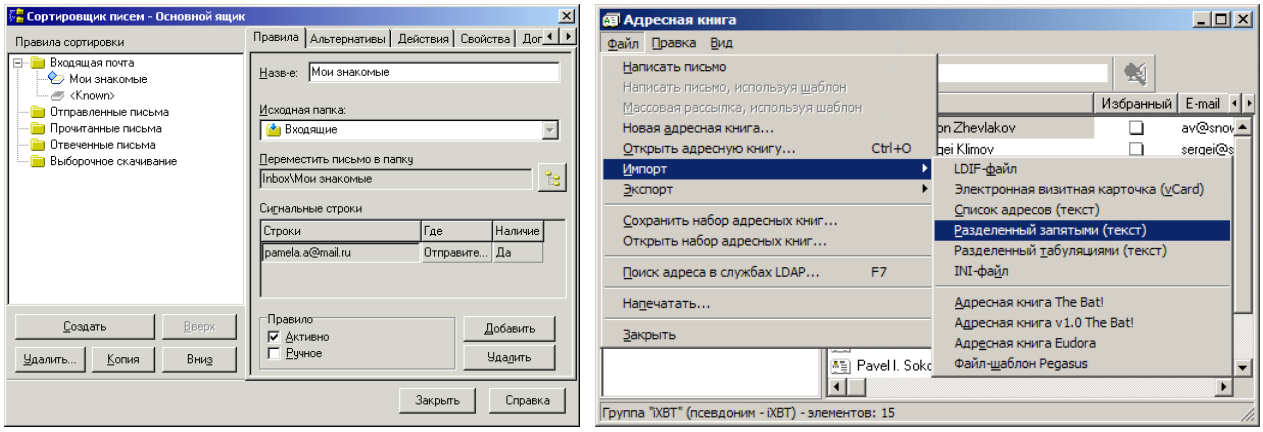


Рисунок 3.63 – Правила роботи клієнта e-mail

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Теоретические основы передачи данных. Часть 1. Киев : КВИУС, 1989. 194 с.
2. Теоретические основы передачи данных. Часть 2. Киев : КВИУС, 1991. 342 с.
3. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб : Питер, 2010. 984 с.
4. Лагутенко О.Н. Современные модемы. Спб. : Лань, 2002. 343 с.
5. Щелованов Л.Н. Системы факсимильной связи. Л. : ЛИЭС, 1991. 46 с.
6. Захарченко Н.В., Филатов Г.Г., Йона Л.Г., Киреев И.А. Факсимильная система связи : учебное пособие. Одесса : УГАС им. А.С. Попова, 2001. 28 с.
7. Программа сетевой академии CISCOCCNA 1 и 2. М. : Вильямс, 2006. 1168 с.
8. Программа сетевой академии CISCOCCNA 3 и 4. М. : Вильямс, 2008. 876 с.
9. Цымбал В.П. Теория информации и кодирование. К. : Вища школа, 1982. 304 с.
10. Скалин Ю.В. Цифровые системы передачи. М. : Радио и связь, 1988. 272 с.
11. Банкет В.Л. Завадостійке кодування в телекомунікаційних системах : навчальний посібник. Одеса : ОНАЗ ім. О. С. Попова, 2011. 100 с.
12. Ватолин Д. и др. Методы сжатия данных.Устройство архиваторов сжатие изображений и видео. М. : ДИЛОГ-МИФИ, 2002. 384 с.
13. Хилл Брайан, Вильямс К.. Полный справочник по Cisco. М. : С-Пб., 2004. 1079 с.
14. HSRP. WEB-ресурс: http://xgu.ru/wiki/HSRP.
15. HSRP в Cisco. WEB-ресурс:http://xgu.ru/wiki/HSRP_%D0%B2_Cisco.
16. Агрегирование каналов. WEB-ресурс: http://xgu.ru/wiki/link_aggregation.
17. Агрегація каналів. WEB-ресурс: https://uk.wikipedia.org/wiki/ Агрегація_каналів.
18. Буров Є. Комп'ютерні мережі. Львів. : Бак, 2003. 584 с.
19. Романов А.И. Телекомунікаційні мережі та управління. Київ : ВПЦ "Київський університет", 2003. 247 с.
20. Зубарев Ю.Б. Передача изображений. М. : Вища школа, 1990.
21. Инструкция по эксплуатации факсимильного аппарата KX-FT72.
22. Информационная база специальной кафедры № 3 (локальный доступ).

ПРИМІТКИ