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.

ТЕЛЕКОМУНІКАЦІЙНІ ТА ІНФОРМАЦІЙНІ МЕРЕЖІ

НАВЧАЛЬНИЙ ПОСІБНИК

*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)

Рецензенти: д.т.н., професор *Єрохін* Віктор Федорович, завідувач 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. Телекомунікаційні та інформаційні мережі: навчальний посібник. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2021. 250 с.

Навчальний посібник відповідає змісту навчальної дисципліни "Телекомунікаційні та інформаційні мережі", охоплює описання характеристик, варіантів структурної побудови та архітектурного описання, а також основних технологій і протоколів сучасних телекомунікаційних та інформаційних мереж.

Даний конспект навчальний посібник призначений для підготовки та проведення навчальних занять для курсантів (студентів), які навчаються в Інституті за спеціальністю 172 "Телекомунікації та радіотехніка", галузі знань 17 "Електроніка та телекомунікації"

УДК 621.396

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

CDP	–	Cisco Discovery Protocol – закритий протокол другого рівня
STP	–	Spanning Tree Protocol – мережевий протокол, що працює на другому рівні моделі OSI
ACL	–	Access Control List – список прав доступу до об’єкта
NAT	–	Network Address Translation – це механізм у мережах TCP/IP, котрий дозволяє змінювати IP-адресу у заголовку пакунку
PAT	–	Port Address Translation – це можливість мережевих пристроїв, яка транслює TCP або UDP зв'язки
AAA	–	Authentication, Authorization, Accounting – використовується для опису процесу надання доступу до комп'ютерної мережі та контролю за ним
RADIUS	–	Remote Authentication Dial-In User Service – протокол передачі даних що використовується в комп'ютерних мережах для автентифікації
TACACS+	–	Terminal Access Controller Access Control System plus – сеансовий протокол, результатом якого є TASACS, виробник Cisco
SSH	–	Secure SHell – мережевий протокол рівня застосунків, що дозволяє проводити віддалене управління комп'ютером і тунелювання TCP-з'єднань
ICMP	–	Internet Control Message Protocol – мережевий протокол, що входить в стек протоколів TCP/IP
VPN	–	Virtual Private Network – узагальнена назва технології, яка дозволяє створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри
MPLS	–	Multiprotocol Label Switching – механізм передачі даних, який емулює різні властивості мереж з комутацією каналів через мережі з комутацією пакетів
GMPLS	–	Generalized Multi-Protocol Label Switching – узагальнена багатопротокольна комутація по міткам
ATM	–	Asynchronous Transfer Mode – мережева високопродуктивна технологія комутації та мультиплексування
xPON	–	Passive Optical Network – це технологія побудови пасивних оптичних мереж
xDSL	–	Digital Subscriber loop – сімейство технологій, що дають змогу значно розширити пропускну здатність абонентської лінії місцевої телефонної мережі

		шляхом використання ефективних лінійних кодів і адаптивних методів корекції викривлень лінії на базі сучасних досягнень мікроелектроніки і методів цифрової обробки сигналу
TCP/IP	–	Internet Protocol / Transmission Control Protocol – це систематизований стек протоколів, що поділяється на чотири рівні, які корелюються з еталонною моделлю OSI
ТКМ	–	телекомунікаційна мережа
MAC	–	Media Access Control – ідентифікатор, що зіставляється з різними типами устаткування для комп'ютерних мереж
CAM	–	Content Addressable Memory – тип памяті, який порівнює вхідні дані з попередньо завантаженим вмістом блоку CAM та генерує заданий результат залежно від типу CAM
ASIC	–	Application-specific integrated circuit – інтегральна схема, спеціалізована для вирішення конкретного завдання
NIC	–	Network interface controller – периферійний пристрій, що дозволяє комп'ютеру взаємодіяти з іншими пристроями мережі
КЦ	–	комутаційний центр
ПЗ	–	Software – сукупність програм системи оброблення інформації та програмних документів, необхідних для експлуатації цих програм
VLSM	–	Variable Length Subnet Mask – технологія, що дозволяє рекурсивно ділити порції адресного простору на невеликі частини
CIDR	–	Classless Inter-Domain Routing – безкласова міждоменна маршрутизація
ВОЛЗ	–	волоконно-оптичні лінії зв'язку
ОК	–	оптичний кабель
АЛ	–	абонентська лінія
ISDN	–	Integrated Services Digital Network – технологія, яка призначена для забезпечення передачі цифрового сигналу по телефонним каналам з представлення різноманітних служб
FDD	–	Feature Driven Development – ітеративна методологія розробки програмного забезпечення
DMT	–	Discrete Multi Tone – метод розділення сигналу цифрової абонентської лінії (DSL) так, щоб корисний діапазон частот був розділений на 256 діапазонів частот (або каналів) по 4,3125 кГц кожен
QAM	–	Quadrature Amplitude Modulation – різновид

амплітудної модуляції сигналу, яка є сумою двох несучих коливань однієї частоти, але зміщених за фазою один відносно одного на 90 градусів, кожне з яких промодульоване по амплітуді своїм модулюючим сигналом

QPSK – Quadrature Phase-Shift Keying – один з видів фазової модуляції, який використовується для передачі цифрового сигналу

OLT – Optical Line Terminal – оптичний лінійний термінал

ONT – Optical Network Terminal – високопродуктивний багатофункціональний абонентський термінал, призначений для доступу до сучасних послуг телефонії, IPTV, OTT і високошвидкісного Інтернету

ВОСП СР – волоконно-оптичні системи із спектральним розділенням по довжині хвилі

GFP – Generic Framing Procedure – протокол, який перетворює пакетний трафік Ethernet, Fibre Channel або ESCON/FICON в постійний синхронний потік даних, який потрібний для його упакування в контейнери ієрархії PDH

WDM – Wavelength Division Multiplexing – спектральне ущільнення каналів, мультиплексування з спектральним розділенням (мультиплексування з розділенням по довжині хвилі)

EDFA – Erbium Doped Fibre Amplifier – волоконно-оптичний підсилювач на оптичному волокні, легованим іонами ербію

ШЦМІО – широкосмугові цифрові мережі з інтегральним обслуговуванням

BPDU – Bridge Protocol Data Unit – фрейм протоколу управління мережевими мостами, IEEE 802.1d, базується на реалізації протоколу STP

STP – Spanning Tree Protocol – алгоритм протоколу сполучного дерева

BID – Bridge ID – ідентифікатор моста

EAP – Extensible Authentication Protocol – протокол розширеної перевірки автентичності

EAPOL – Extensible Authentication Protocol Over LAN – протокол розширеної перевірки автентичності через локальну мережу, через порт до якого підключений користувач

ВСТУП

Навчальний посібник призначений для підготовки та проведення занять з навчальної дисципліни “Телекомунікаційні та інформаційні мережі” для курсантів (слухачів, студентів), які навчаються за спеціальністю 172 “Телекомунікації та радіотехніка”, галузі знань 17 “Електроніка та телекомунікації”, освітньо-професійної програми бакалаврів “Спеціальні телекомунікаційні системи” денної форми навчання і є навчальною дисципліною обов’язкової професійної та практичної підготовки.

Предметом навчальної дисципліни є вивчення особливостей побудови та оволодіння навичками проектування, експлуатації та аналізу мереж, а також розрахунків характеристик і показників функціонування телекомунікаційних та інформаційних мереж.

Метою навчальної дисципліни є формування у курсантів здатностей:

– здійснювати моделювання технічних об’єктів і технологічних процесів на основі сучасних методів математичного та комп’ютерного моделювання;

– застосовувати методи контролю якості апаратно-програмних засобів спеціальних телекомунікаційних систем, проводити їх сертифікацію та експертизу;

– проектувати мережі передачі даних за заданими показниками основних характеристик;

– проектувати, налаштовувати, контролювати стан та оцінювати ефективність мереж передачі даних;

– брати участь у проектуванні нових (модернізації існуючих) апаратно-програмних засобів спеціальних телекомунікаційних систем.

Згідно з вимогами освітньо-професійної програми курсанти після засвоєння навчальної дисципліни мають продемонструвати такі результати навчання:

знання:

– теоретичних основ побудови телекомунікаційних та інформаційних мереж;

– основних характеристик і показників мереж та методів їх розрахунку;

– основних телекомунікаційних технологій побудови мереж;

– методів синтезу мереж;

– областей використання вивчаємих методів та оцінки складності їх реалізації;

– перспектив розвитку і напрямків вдосконалення телекомунікаційних та інформаційних мереж;

– напрямків вдосконалення методів аналізу та розрахунку основних характеристик і параметрів функціонування телекомунікаційних та інформаційних мереж;

– протоколів налаштування та перевірки зв’язаної мережі з резервуванням;

– варіантів та способів реалізації списків контролю доступу ACL;

– порядку організації аутентифікації, авторизації та обліку діяльності адміністраторів мереж;

вміння:

– виконувати розрахунки основних характеристик телекомунікаційних мереж та їх елементів;

– оцінювати ефективність способів побудови мереж та функціонування їх протоколів і процедур управління;

– самостійно робити інформаційний пошук та порівняльний аналіз структур і характеристик мереж;

– налаштовувати та контролювати роботу протоколів CDP, STP, ACL, NAT, PAT, AAA (LOCAL, RADIUS, TACACS+);

– застосовувати команди та протоколи telnet/ssh та ICMP;

досвід:

– налаштування систем адресування та маршрутизації мереж;

– налаштування в обладнанні Cisco протоколів CDP, STP, ACL, NAT, PAT, AAA (LOCAL, RADIUS);

– проектування та експлуатації локальних мереж органів державного управління.

Науковою основою навчальної дисципліни є теорія побудови телекомунікаційних мереж, теорія реалізації архітектури інформаційних мереж, теорія проектування (синтезу і аналізу) і розрахунку показників функціонування телекомунікаційних мереж.

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.

Успішне вирішення завдань навчальної дисципліни базується на засвоєні курсантами знань та умінь, сформованих у них, в результаті вивчення таких навчальних дисциплін: “Загальна фізика”, “Інформатика”, “Основи теорії кіл”, “Основи теорії телекомунікацій”, “Схемотехніка”, “Телекомунікаційні системи передачі”, “Лінії передачі”, “Системи комутації та розподілу інформації”.

Навчальні дисципліни, які забезпечуються цією навчальною дисципліною – “Системи передачі даних”, “Засоби та комплекси спеціального зв’язку”, “Практичне виконання навчально-бойових задач”, “Навчальні дисципліни з тактико-спеціальної підготовки”.

Навчальна дисципліна спрямована на формування у курсантів твердих знань з теорії побудови та експлуатації телекомунікаційних мереж, архітектури інформаційних мереж, аналізу та синтезу мереж, розрахунків характеристик і показників функціонування телекомунікаційних та інформаційних мереж, а також оволодіння загальними принципами побудови

локальних і глобальних мереж органів державного управління, системами адресування, маршрутизації, управління та формування у курсантів здатностей:

– здійснювати моделювання технічних об'єктів і технологічних процесів на основі сучасних методів математичного та комп'ютерного моделювання;

– застосовувати методи контролю якості апаратно-програмних засобів спеціальних телекомунікаційних систем, проводити їх сертифікацію та експертизу;

– проектувати мережі передачі даних за заданими показниками основних характеристик;

– проектувати, налаштовувати, контролювати стан та оцінювати ефективність мереж передачі даних;

– брати участь у проектуванні нових (модернізації існуючих) апаратно-програмних засобів спеціальних телекомунікаційних систем.

Змістовно навчальна дисципліна (кредитний модуль) згідно з робочим навчальним планом складається з наступних тем:

Тема 1. **Побудова телекомунікаційних та інформаційних мереж**

Узагальнена структура телекомунікаційної мережі. Загальні вимоги до зв'язку. Види зв'язку. Призначення і склад телекомунікаційних мереж. Принципи створення Глобальної інформаційної інфраструктури. Інформаційні мережі. Морфологічне описання телекомунікаційної мережі. Функціональне описання телекомунікаційних мереж. Структурно-топологічне описання телекомунікаційних мереж.

Загальні поняття про архітектуру мереж. Функціональна модель інформаційної мережі. Програмна структура мережі. Протокольна модель мережі. Модель реалізації інформаційної мережі.

Характеристика та призначення рівневих протоколів моделі взаємодії відкритих систем. Рівні еталонної моделі взаємодії відкритих систем. Структура повідомлення у моделі ВВС. Протоколи в інформаційних мережах та зв'язок між рівнями. Обладнання інформаційних мереж за моделлю ВВС.

Тема 2. **Основні характеристики, аналіз і синтез телекомунікаційних мереж**

Якість обслуговування в телекомунікаційних мережах. Пропускна здатність телекомунікаційних мереж. Живучість телекомунікаційних мереж. Надійність функціонування телекомунікаційних мереж.

Постановка задач розрахунку основних параметрів ТКМ. Методи розрахунку параметрів ТКМ.

Поняття про задачі синтезу та аналізу. Задачі синтезу телекомунікаційних мереж. Задачі аналізу телекомунікаційних мереж. Синтез зв'язаної мережі мінімальної вартості за алгоритмом Пріма. Синтез зв'язаної мережі мінімальної вартості за алгоритмом Краскела. Визначення оптимального місця розташування опорного вузла в кабельній мережі

абонентського доступу. Визначення оптимального місця розташування базової станції в мережі стаціонарного радіо доступу. Визначення циклу найменшої довжини для організації транспортного кільця. Знаходження найкоротшого шляху в зв'язаній мережі за алгоритмом Дейкстри. Знаходження найкоротшого шляху в зв'язаній мережі за алгоритмом Белмана-Форда. Визначення множини шляхів заданої кількості транзитів.

Тема 3. **Принципи функціонування телекомунікаційних та інформаційних мереж і керування ними**

Структура і функціонування локальних мереж. Основні технології локальних мереж і їх загальна характеристика. Структуризація локальних мереж. Адресування в телекомунікаційних та інформаційних мережах. Поняття комутації в мережах.

Порядок та практика використання програми емуляції IP-мереж в програмному середовищі Cisco Packet Tracer.

Виготовлення кабелю (пач-корд) для з'єднання обладнання локальної мережі. Виконання з'єднання комп'ютерів у локальну мережу та налаштування стеку протоколів TCP/IP.

Задачі систем управління телекомунікаційних та інформаційних мереж. Структура реалізації протоколів управління ТКМ. Загальна характеристика засобів моніторингу.

Маршрутизація у телекомунікаційних та інформаційних мережах. Протоколи маршрутизації IP-мереж. Команди практичної реалізації основних протоколів маршрутизації в IP-мережах.

Конфігурування інтерфейсів і протоколів маршрутизації. Порядок проектування локальної мережі органу державного управління. Порядок емуляції локальної мережі органу державного управління в програмному середовищі Cisco Packet Tracer.

Тема 4. **Загальна характеристика телекомунікаційних технологій**

Технології глобальної мережі Інтернет. Структура всесвітньої мережі. Технології транспортних телекомунікаційних мереж.

Технології xDSL та xPON

Принципи функціонування систем ATM. Сутність технології ATM. Еталонна модель протоколів ATM. Рівні та площини протоколів ATM. Площини моделі керування ATM та їх функції

Мережі з використанням технології MPLS. Технологія GMPLS. Мультисервісні транспортні мережі. Структура та використання заголовків в сегменті MPLS. Основні операції з мітками. Маршрутизація в сегменті MPLS. Віртуальні приватні мережі MPLS (VPN MPLS).

Тема 5. **Протоколи налаштування та перевірки зв'язаної мережі з резервуванням**

Основні задачі адміністрування мереж та шляхи їх рішення. Налаштування та використання протоколів аналізу та перевірки мереж (CDP,

telnet/ssh, ICMP (команди ping та tracert)). Протокол взаємодії мереж 2 рівня STP. Моделювання мережі з замкненими контурами у середовищі Packet Tracer. Налаштування мережі 2 рівня з замкненими контурами та резервуванням

Тема 6. **Реалізація та застосування списків контролю доступу ACL**

Реалізація контролю доступу з використанням ACL. Моделювання та налаштування мережі з доступом, що обмежений засобами ACL. Протоколи перетворення адрес NAT та PAT. Моделювання мережі з протоколами перетворення адрес NAT та PAT

Тема 7. **Аутентифікація, авторизація та облік діяльності адміністраторів мереж**

Організація процедур аутентифікації, авторизації та обліку діяльності адміністраторів мереж. Варіанти реалізації протоколів AAA. Моделювання та налаштування мереж з доступом адміністраторів через служби AAA

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

1) роботу на практичних заняттях: **4** відповіді (в кожного курсанта мінімум) на **15** групових практичних та семінарських заняттях (за умови, що на одному занятті опитуються 7…8 курсантів при максимальній чисельності групи 25…30 осіб – (15 пз × 7…8 курсантів):(25…30 курсантів) ≈ 4 відповіді);
2) конспект на практичному занятті № 4/7т;
3) оцінки за виконання та захист лабораторних робіт: **3** оцінки (заняття № 3/8, 3/11 та 4/8);
4) оцінки за виконання схем-моделей мереж на комп'ютерних практикумах (заняття № 5/2, 5/4, 6/3, 6/6 та 7/3): **5** оцінок (в кожного курсанта) на **5** комп'ютерних практикумах;
5) **1** модульна контрольна робота (МКР), яка складається з 7 письмових експрес-контролів: за темами 1-7 (кожний ПЕК виконується протягом 15…20 хвилин на визначеному практичному занятті).

Робота курсанта в семестрі оцінюється наступним чином:

1. Робота на практичних заняттях (кількість відповідей в кожного курсанта мінімум – **4**).

Ваговий бал – **5**.

Максимальна кількість балів – **20**.

Критерії оцінювання:

5 – *все вірно, відповідь без зауважень (не менш ніж 90% від потрібної інформації), традиційна оцінка – відмінно;*

4 – *вірно, але не повністю, відповідь з незначними помилками (не менш ніж 75% від потрібної інформації) – традиційна оцінка добре;*

3 – *відповідь має певні недоліки, потребує корективи та поправки з боку викладача або курсантів (не менш ніж 60% від потрібної інформації), традиційна оцінка – задовільно;*

1…2– *відповідь має явні недоліки, потребує значні корективи та поправки з боку викладача, хоча пояснення в вірному напрямку, традиційна оцінка – задовільно з мінусом;*

0 – *не відповідає вимогам оцінки "задовільно", традиційна оцінка – незадовільно.*

2. Оцінка за конспект на практичному занятті № 4/7т

Ваговий бал – **5**.

Максимальна кількість балів – **5**.

Критерії оцінювання:

5 – *все вірно, повний та якісний конспект (не менш ніж 90% від потрібної інформації), традиційна оцінка – відмінно;*

4 – *все вірно, конспект повний, але виконаний неякісно (не менш ніж 75% від потрібної інформації) – традиційна оцінка добре;*

3 – *конспект має певні недоліки, потребує корективи та поправки (не менш ніж 60% від потрібної інформації), традиційна оцінка – задовільно;*

0 – *не відповідає вимогам оцінки "задовільно" – незадовільно.*

3. Оцінки за виконання та захист лабораторних робіт (заняття № 3/8, 3/11 та 4/8) (кількість оцінок в кожного курсанта – **3**).

Ваговий бал – **5**.

Максимальна кількість балів – **15**.

Критерії оцінювання:

5 – *все вірно, виконання та захист без зауважень (не менш ніж 90% від потрібної інформації), традиційна оцінка – відмінно;*

4 – *вірно, але не повністю, виконання або захист з незначними помилками (не менш ніж 75% від потрібної інформації) – традиційна оцінка добре;*

3 – *виконання або захист мають певні недоліки, потребують коректівів та поправок (не менш ніж 60% від потрібної інформації), традиційна оцінка – задовільно;*

0 – *не відповідає вимогам оцінки "задовільно" – незадовільно.*

4. Оцінки за виконання схем-моделей мереж на комп'ютерних практикумах (**5** оцінок).

Ваговий бал – **5**.

Максимальна кількість балів – **25**.

Критерії оцінювання:

5 – *все вірно, виконання без зауважень (не менш ніж 90% від потрібної інформації), традиційна оцінка – відмінно;*

4 – *вірно, але не повністю, виконання з незначними помилками (не менш ніж 75% від потрібної інформації) – традиційна оцінка добре;*

3 – *виконання має певні недоліки, потребує корективів та поправок (не менш ніж 60% від потрібної інформації), традиційна оцінка – задовільно;*

0 – *не відповідає вимогам оцінки "задовільно" – незадовільно.*

5. Модульний контроль (кількість – **1**)

Ваговий бал – **35**.

Максимальна кількість балів – 35.

МКР складається з **7** письмових експрес-контролів, які виконуються протягом 15…20 хвилин на відповідному практичному занятті. Кожний ПЕК оцінюється максимум в 5 балів (2 питання – по 2,5 балів кожне). Кількість балів за МКР складає суму кількості балів ПЕК (**35** = **5** × **7**), що входять до його складу.

Критерії оцінювання окремого питання ПЕК:

2,5(x2) – *відповідь на питання вірне, без зауважень (не менш ніж 90% від потрібної інформації), традиційна оцінка – відмінно;*

2(x2) – *відповідь з помилками (не менш ніж 75% від потрібної інформації) – традиційна оцінка добре;*

1,5(x2) – *відповідь із значними недоліками, потребує корективів (не менш ніж 60% від потрібної інформації), традиційна оцінка – задовільно;*

0 – *не відповідає вимогам оцінки "задовільно", традиційна оцінка – незадовільно.*

Розрахунок шкали (R) рейтингу:

Максимальний рейтинг за семестр складає **100 балів,** сума вагових балів контрольних заходів протягом семестру складається таким чином:

R_C= 20 (4 відповіді ×5) + 5 (конспект 5/7) + 15 (3 ЛР ×5) + 25 (5 схем ×5) + 35 (1 МКР ×35) = 20+5+15+25+35 = 100

Штрафні та заохочувальні бали: Сума як штрафних, так і заохочувальних балів не має перевищувати 0,1×R_C.

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, затримку із захистом лабораторної роботи (схеми-моделі, конспекту) можна отримати штрафні (від'ємні бали) відповідно ваговим балам за видами занять.

Необхідною умовою допуску до заліку є:

1. Виконання та захист 3 (трьох) звітів лабораторних робіт.
2. Відпрацювання конспекту.

3. Виконання та захист 5 (п’яти схем-моделей).
4. Подача до захисту курсової роботи.

Курсанти, які не виконали умов допуску до заліку не допускаються і повинні підвищити свій рейтинг.

Курсанти, які набрали впродовж семестру необхідну кількість балів (*RD* ≥ **0,6***R*) (**≥60 балів**), мають можливість отримати загальну оцінку автоматично, відповідно до набраного рейтингу (див. табл. 1.1).

Таблиця 1.1

Сумарний рейтинг RD			**Оцінка *ECTS* та визначення**
Бали			
95	…	100	відмінно
85	…	94	дуже добре
75	…	84	добре
65	…	74	задовільно
60	…	64	достатньо

Якщо курсанта не влаштовує набрана кількість балів, він має можливість її підвищити, шляхом виконання залікової контрольної роботи. Залік письмовий виконується за жорсткою системою (тобто результати навчання в семестрі не враховуються).

Максимальна кількість балів, яку може отримати курсант за залікову контрольну роботу **100 балів (в білеті 4 питання – кожне питання по 25 балів)**. Підсумкова оцінка за залік виставляється згідно з табл. 1.2.

Таблиця 1.2

Сумарний рейтинг RD	**Оцінка**
95…100	відмінно
85…94	дуже добре
75…84	добре
65…74	задовільно
60…64	достатньо
Сумарний рейтинг < 60	незадовільно

Примітки:

- положення про рейтингову систему оцінки успішності доводиться на першому занятті з дисципліни;
- попередня рейтингова оцінка (R_C) з кредитного модуля (дисципліни) доводиться до курсантів на останньому занятті;
- календарний контроль курсантів з навчальної дисципліні проводиться викладачами за значенням поточного рейтингу курсанта (r_{ct}) на час атестації t. Якщо значення цього рейтингу не менше 50% від максимально можливого (R_{ct}) на час атестації $r_{ct} \geq 0{,}5R_{ct}$, курсант вважається задовільно атестованим, з виставленням в атестаційній відомості “а”. Інакше в атестаційній відомості виставляється “на”;
- календарний контроль проводиться згідно графіка-календаря освітнього процесу ІСЗЗІ КПІ ім. Ігоря Сікорського на навчальний рік.

РОЗДІЛ 1
ПОБУДОВА ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНФОРМАЦІЙНИХ МЕРЕЖ

1.1. Основи побудови телекомунікаційних мереж

1.1.1. Структура телекомунікаційних (інформаційних) мереж

Для виконання задач, покладених на телекомунікаційну мережу, у її склад входять кінцеві пристрої, що одержали назву терміналів чи термінального устаткування, лінії зв'язку і комутаційні центри. Кожний з елементів має чітко визначені функції і при побудові може використовувати різні принципи. Будучи технічними пристроями різного ступеня складності, вони можуть розглядатися як функціонально – відособлені системи, кожна з яких вирішує визначений перелік задач у відповідності зі своїми критеріями оптимальності. Разом з тим, виконання поставлених перед телекомунікаційною мережею задач можливо лише при спільному їхньому використанні. Тоді як *визначення* телекомунікаційної мережі можна використовувати наступне [2]*:* ***телекомунікаційною мережею називається*** сукупність термінального устаткування, комутаційних центрів та ліній і каналів зв'язку, що їх з'єднують, об'єднаних загальною метою функціонування.

Основним призначенням телекомунікаційної мережі є доведення необхідного обсягу інформації відповідно до заданих адрес й з необхідними показниками якості обслуговування.

У загальному випадку телекомунікаційну мережу можна представити у вигляді узагальненої структури, що містить 4 макрорівні (рисунок 1).

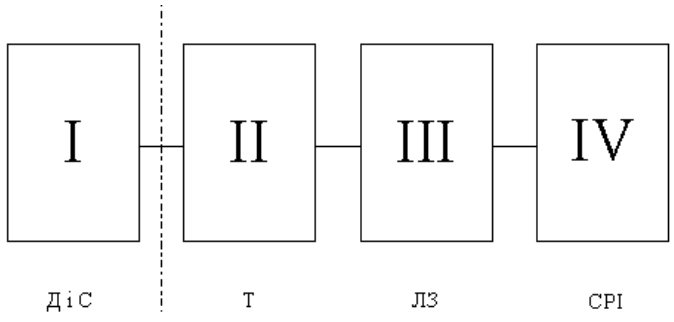


Рисунок 1.1 – Узагальнена структура телекомунікаційної мережі

Перший рівень – це джерела і споживачі інформації. Вони користуються послугами ТКМ і створюють потоки повідомлень різного виду і призначення. Саме вони визначають вимоги до ТКМ по доставці й обробці інформації з дотриманням визначених якісних і кількісних показників. Це зовнішнє середовище ТКМ.

Другий рівень – це термінали, кінцеві пристрої різного призначення. У загальному випадку вони являють собою інструмент, за допомогою якого джерела і споживачі інформації здійснюють введення/вивід повідомлень. При цьому, під повідомленням розуміється сукупність таких даних, що передані засобами телекомунікацій і мають ознаки початку і кінця.

Третій рівень – це лінії зв'язку. Вони забезпечують доставку повідомлень на необхідні відстані у вигляді сигналів електрозв'язку.

Четвертий рівень – це системи розподілу інформації (СРІ). Вони забезпечують розподіл повідомлень відповідно до зазначеної у заявці адреси і є ланкою, що поєднує ТКМ та всю телекомунікаційну систему в цілому. Основним елементом СРІ є різного роду комутаційні центри (КЦ) . Вони багато в чому визначають показники якості функціонування ТКМ.

Оптимальність побудови технічних пристроїв на кожному рівні, можливості їх адаптації до змін внутрішніх і зовнішніх параметрів, надійність і живучість багато в чому визначають можливості телекомунікаційної мережі.

Під поняттям „**Інформаційна мережа**" будемо розуміти сукупність територіально рознесених прикінцевих систем і об'єднуючої їх телекомунікаційної мережі, що забезпечує доступ прикладних процесів (сервісних послуг) будь-якої з цих систем до всіх ресурсів інформаційної мережі і їхнє спільне використання.

Прикладний процес (***application process***) – це процес в прикінцевій системі мережі, що виконує оброблення інформації для конкретної послуги зв'язку або додатку.

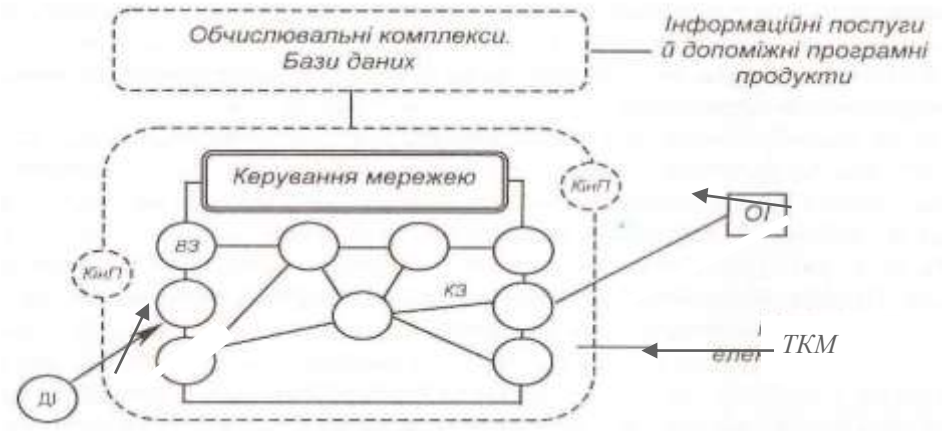


Рисунок 1.2 – Схема інформаційної мережі:
КінП – кінцевий пункт; КЗ – канал зв'язку; ВЗ – вузол зв'язку; ДІ – джерело інформації; ОІ – одержувач інформації

Кінцеве обладнання (ДСТУ-2615-94) – обладнання користувача, що забезпечує функції необхідні для дії протоколів користувач-мережа. Користувач (мережі зв'язку) – особа чи пристрій, делегований споживачем, які користуються послугами мережі зв'язку.

Кінцевими системами інформаційної мережі можуть бути:

– **термінальні системи** (***terminal system***) – забезпечують доступ до мережі та її ресурсів;

– **робочі станції** (***server, host system***) – надають мережний сервіс (керування доступом до файлів, програм, тощо);

– **адміністративні системи** (***management system***) – здійснюють керування мережею і окремими її ділянками (елементами).

Ресурси інформаційної мережі поділяються на:

– інформаційні;

– ресурси оброблення і зберігання даних;

– програмні;

– комунікаційні.

Інформаційні ресурси представляють собою інформацію і знання накопичені в розподілених банках в інтересах системи державного управління, використовуючи які посадові особи здійснюють управління. Ці ресурси фактично визначають цінність інформаційної мережі і повинні не тільки постійно створюватися і розширюватися, а і вчасно поновлюватись (транзакції, реплікації).

Ресурси оброблення і зберігання даних – це система формування і організації розподіленого банку даних органів державного управління, система хешування інформації, служба каталогів, доступу і захисту даних; це продуктивність серверів і процесорів мережних комп'ютерів й обсяги їхніх запам'ятовуючих пристроїв, а також час, впродовж якого вони використовуються.

Програмні ресурси являють собою програмне забезпечення як елементів, так і всієї телекомунікаційної мережі, мережні операційні системи, мережні стеки протоколів, служби (**NFS**, **DNS** і т.і.) програмне забезпечення надання послуг і додатків користувачам (**SMTP**, **HTTP**, **FTP**, ***Telnet***, **SNMP** і т.і.). Це програмні засоби перетворення форматів повідомлень, що передаються, криптозахисту інформації, аутентифікації (електронний цифровий підпис, що засвідчує істинність документу).

Комунікаційні ресурси – це засоби, що забезпечують транспортування інформації з заданою якістю та перерозподіл потоків у комунікаційних центрах. Вони класифікуються відповідно до типу телекомунікаційних мереж: ресурси комутованої телефонної мережі загального користування (ТФЗК); ресурси мережі передачі даних; ресурси мобільної мережі; ресурси магістральної мережі; ресурси локальних мереж органів державного управління; ресурси мереж доступу, тощо.

1.1.2. Загальні вимоги до зв'язку. Види і роди зв'язку

З боку споживачів до зв'язку висувається ряд вимог, основними з яких є:

1. Доставка повідомлень по заданій адресі.

Помилкова доставка повідомлення може призвести не тільки до втрати інформації, але і можливо небажане розголошення відомостей, що містяться в повідомленні.

2. Забезпечення передачі заданого обсягу інформації.

Зменшення обсягу переданої інформації від необхідного може різко знизити інформативність переданого повідомлення.

3. Своєчасність доставки повідомлень.

Затримка в передачі повідомлення понад припустиму норму веде до втрати цінності інформації, що міститься в ньому, а у визначених умовах можлива дезорганізація управління.

4. Забезпечення заданої вірогідності передачі інформації.

Викривлення, допущені при передачі інформації, можуть привести до перекручення змісту переданого повідомлення.

5. Дотримання необхідної дисципліни обслуговування.

Відповідно до положення, яке займає абонент в ієрархії системи управління, чи категорією терміновості інформації, що міститься в повідомленні, повинні бути забезпечені пріоритети в алгоритмах обробки інформації.

У залежності від виду переданого повідомлення значимість тих чи інших вимог може змінюватися. **Вид зв'язку** – це класифікаційне угруповання зв'язку, виділена по виду переданого повідомлення (кінцевого обладнання або засобу зв'язку).

Основними видами зв'язку, поширеними в даний час на Україні є телефонний, передача даних і факсимільний.

Надання абонентам того чи іншого виду зв'язку обумовлюється:

1.Зручністю користування і доступністю того чи іншого термінала для передачі необхідного виду інформації.

2.Характером повідомлень, що підлягають передачі.

3.Способами збереження і подальшого використання повідомлень.

Повідомлення різних видів зв'язку висувають специфічні вимоги до їхньої передачі.

Так, *телефонні повідомлення* не припускають помітних затримок [3] у передачі окремих елементів повідомлення (звуків слів, фраз). При цьому думки фахівців про величину припустимого значення T неоднозначні. В одних джерелах указується, що при $T \le 600$ мс якість діалогу істотно не погіршується, а при $T > 900$ мс діалог стає неможливий. В інших джерелах відзначається, що припустиме значення T знаходиться в діапазоні від 500 до 1000 мс, тому що людині властиво адаптуватися до таких затримок. У третіх, уточнюється про доцільність величини $T \le 300$ мс, тому що при $300 \text{ мс} < T \le 600$ мс великому числу абонентів складно вести діалог, а при $T > 1000$ мс – діалог не можливий. Більшість фахівців сходиться, що найбільше доцільно прийняти: $T \le 300$ мс. При цьому в обов'язковому порядку повинна зберігатися природна послідовність проходження мовних елементів, обумовлена специфікою ведення переговорів абонентами.

Разом з тим велика надмірність телефонного повідомлення допускає значну (у порівнянні з повідомленнями інших видів зв'язку) величину втрат його елементів без істотного зниження вірогідності передачі (розбірливості і натуральності).

Повідомлення передачі даних, навпаки, вимагають більшої вірогідності передачі, але часто допускають значну затримку як окремих елементів (кілька секунд і більш), так і повідомлень у цілому. Приклад тому – телеграма.

Вимоги до вірогідності передачі повідомлень даних видів зв'язку визначаються рядом факторів. Так, при передачі повідомлень, що несуть змістовну інформацію, ці вимоги можуть знижуватися. А при передачі цифрових даних, що включають у свій склад ключову інформацію, координати крапок на місцевості і т.д. вимоги до вірогідності дуже високі.

Обсяги переданої інформації з кожного виду зв'язку неоднакові. З усіх видів зв'язку, що забезпечують обмін інформацією між споживачами, найбільший обсяг передається за допомогою телефонного зв'язку. Це зв'язано з тим, що мовне повідомлення передає кілька видів інформації: змістовну (текст повідомлення), інформацію про особу, яка говорить (ознаки, що дозволяють довідатися хто говорить по голосу), і інформацію про емоційні фактори (інтонаційні ознаки). У зв'язку з цим даний вид зв'язку найбільш наближений до особистого спілкування і має саме широке використання.

Неоднакові і темпи росту обсягів інформації, передача якої забезпечується різними видами зв'язку. Бурхливий розвиток останнім часом засобів обчислювальної техніки й автоматизованих систем управління обумовлює тенденцію прискорення росту обсягу повідомлень даних.

Використання телефонного зв'язку, у порівнянні з іншими видами зв'язку має найбільше наближення до особистого спілкування. При цьому застосовуються порівняно прості кінцеві пристрої. Це забезпечує абоненту зручність користування засобами зв'язку й оперативність введення/виводу інформації. У зв'язку з цим при забезпеченні повсякденного обміну інформацією між людьми телефонному зв'язку приділяється першочергова увага.

Передача даних, телеграфний і факсимільний зв'язок відносяться до документальних видів зв'язку. Передані і прийняті повідомлення можуть мати вигляд телеграм (кодограм, шифрограм) або прямих переговорів між абонентами і документуватися на відповідному носії. У більшості випадків абонент уводить телеграфне повідомлення в систему через третіх осіб (операторів). При цьому від моменту виникнення заявки на передачу повідомлення до вручення телеграми адресату проміжок часу може складати від кількох секунд до декількох днів. Це дозволяє трохи спростити системи передачі і розподілу інформації і підвищити ефективність використання каналів ТКМ.

Обмін інформацією між ЕОМ (міжмашинний обмін), а також між людиною й ЕОМ сприяв широкому використанню передачі даних. Дані

мережі також мають свою специфіку, яка залежить від того, чи входять ЕОМ до складу єдиного обчислювального центру або є елементами автоматизованих систем управління різного призначення, або розподіленої бази даних і т.д.

Рід зв'язку – класифікаційне угруповання зв'язку, виділене по середовищу поширення сигналів і типу лінійних засобів.

Розрізняють наступні роди зв'язку:

- радіозв'язок;
- радіорелейний зв'язок;
- тропосферний зв'язок;
- супутниковий зв'язок;
- проводовий зв'язок;
- волоконно-оптичний зв'язок;
- сигнальний зв'язок.

1.1.3. Архітектура мереж

Архітектурою називається системний опис мережі, що відображає всю різноманітність її елементів, зв'язків між ними і правил взаємодії.

Під системним описом розуміють багаторівневий опис об'єкта у вигляді моделей, кожна з яких відбиває об'єкт у певному аспекті його розгляду (рівня абстрагування).

Модель – це таке відображення об'єкта, яке дозволяє досліджувати його основні елементи, не відволікаючись на несуттєві, з точки зору поставленої мети, деталі. Рівні абстрагування звичайно розташовуються в ієрархічному порядку (підпорядкування за старшинством).

Модельний опис мережі як складної системи (опис її архітектури) можна здійснити лише єдиним шляхом – розчленуванням її на велику кількість структур, кожна з яких відбиває взаємозв'язок певної групи елементів, виділених на певному рівні розгляду мережі.

Таким чином, архітектура є містке поняття, яке відбиває взаємозв'язок різноманітних структур мережі:

- конфігурації ліній, що об'єднують її пункти (топології);
- функціональної структури, що пояснює логіку роботи мережі;
- програмної структури, що характеризує склад надзвичайно складного і багатоцільового програмного забезпечення мережі;
- протокольної моделі мережі, що описує правила встановлення зв'язку і забезпечення інформаційного обміну;
- фізичної структури, що дозволяє оцінити фізичні ресурси мережі, типи використовуваного обладнання.

Функціональна модель являє собою абстрактний опис мережі на **логічному рівні**, що не залежить від принципів її фізичної реалізації. Така модель відображає взаємозв'язок виконуваних в мережі функцій.

Розрізнюють такі основні типи виконуваних в інформаційній мережі функцій:

– **прикладні** функції – об'єкти додатків користувачів і адміністрації мережі;

– функції **керування послугами** – об'єкти, що дозволяють будувати послуги з компонентів послуг і пов'язаних з ними модулів ресурсів і керувати взаємодією користувачів з цими послугами;

– функції **адміністративного керування мережею** – об'єкти, що здійснюють керування всіма іншими функціями;

– функції **обробки і зберігання даних** – об'єкти та модулі, що забезпечують виклик і керування об'єктами додатків, їхню взаємодію, а також вилучення запитуваних даних або введення їх у базу даних;

– **комунікаційні** функції – об'єкти та модулі, що забезпечують транспортування і керування потоками інформації (при їхньому перерозподілі в комунікаційних вузлах).

Аналіз **програмної структури** дозволяє розглянути ієрархію мережного програмного забезпечення. Елементами цієї структури є програмні модулі, в яких реалізовано логічні елементи мережі.

Ієрархія програмного забезпечення (ПЗ) може бути подана в такому вигляді:

– прикладне ПЗ;
– проміжне ПЗ;
– базове ПЗ.

У **прикладному ПЗ** реалізовано об'єкти додатків. Розрізняють два типи додатків, що впливають на структуру організації ПЗ – це локально обмежені і розподілені додатки. **Локально обмежений додаток** інсталюється, викликається, керується і виконується повністю в межах однієї прикінцевої системи і не потребує залучення комунікаційних функцій. **Розподілений додаток** складається з декількох компонентів, що можуть виконуватися в різних прикінцевих системах і, отже, вимагають організації взаємодії цих прикінцевих систем.

Проміжне ПЗ реалізує в мережі функції керування послугами і функції адміністративного управління мережею. Об'єкти обох груп аналогічно до компонентів розподільних додатків взаємодіють за допомогою комунікаційних функцій. За допомогою проміжного ПЗ в мережі конкретизуються концепції інтелектуальних мереж та загальної схеми багаторівневого керування мережами **TMN** (***Telecommunication Management Network***), які стали вже досить відомими.

Базове ПЗ призначене для забезпечення об'єктами прикладного ПЗ і проміжного ПЗ можливості виконання і взаємодії з іншими об'єктами за допомогою забезпечення середовища взаємодії з комунікаційними функціями і логічними інтерфейсами користувачів. Організація середовища здійснюється уніфікованими програмними комплексами, які називаються **мережними та міжмережними операційними системами**. Стандартами де-факто на сьогоднішній день в цьому плані стали мережні системи **UNIX** та

Windows* NT**, а також міжмережні системи – **IOS** (Interworking Operation System***) фірми ***Cisco Systems*** та **NOS** (***Networking Operation System***) фірми ***Motorola***.

Протокольна модель описує правила роботи мережі на рівні взаємодії об'єктів і логічних модулів при реалізації основних процесів передавання й оброблення інформації. В цій моделі всі правила (протоколи) взаємодії згруповано за їх функціональним призначенням в окремі групи – протокольні блоки. Протокольні блоки розташовуються в ієрархічному порядку, і кожний з них представляє собою перелік протоколів взаємодії об'єктів певного рівня (рисунок 1.3).

При виконанні задачі **N**-рівня беруть участь об'єкти **N**-рівня, що виконують локальний комплекс функцій даного рівня. Однак протокольні блоки розбиті за рівнями таким чином, що можливість виконання задачі **N**-рівня цілком залежить і забезпечується участю об'єктів (**N-1**)-го рівня і т. д. Таким чином, об'єкти **N**-рівня залучають у взаємодію (**N-1**)-рівень, (**N-1**) – об'єкти (**N-1**)-рівня – з (**N-2**) – об'єктами і т. д. Кожний нижчестоящий рівень надає сервіс вищім рівням.

Будь-який об'єкт **N**-рівня при переході в активний стан видає інформацію двох видів:

1) інформація, що передається поміж об'єктами **N**-рівня (дані користувача) і не пов'язана з операціями „з'єднання" цих об'єктів;

2) керуюча інформація, призначена для (**N-1**)-рівня, за допомогою, якої здійснюється координація процедур „з'єднання" об'єктів **N**-рівня.

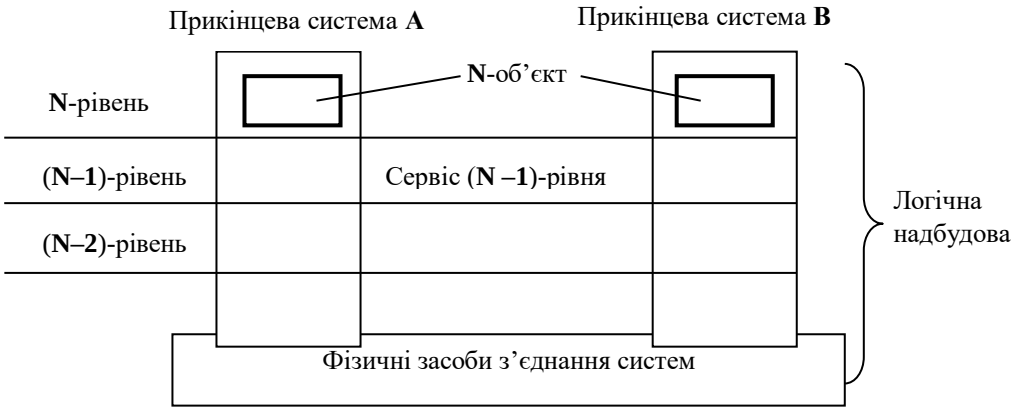


Рисунок 1.3 – Принцип побудови протокольних блоків

Усі правила взаємодії об'єктів у протокольній моделі визначають стандарти для конкретної мережі і класифікуються як протоколи (стандарти взаємодії об'єктів одного рівня) та інтерфейси (стандарти взаємодії об'єктів сусідніх рівнів). Ці поняття нам вже знайомі з попередніх моделей.

Міжнародна організація стандартів **ISO**, аналізуючи досвід створення інформаційних мереж, і особливо комп'ютерних мереж у багатьох країнах світу, розробила концепцію побудови мереж, яка названа **архітектурою відкритих систем**. Відповідно до цієї концепції було створено протокольну модель, що дозволила ввести міжнародні стандарти, які визначають і

регламентують розробки систем і мереж. Ця модель дістала назву **еталонної моделі взаємодії відкритих систем** (**ВВС**). Системи і мережі, що задовольняють вимогам і стандартам еталонної моделі ВВС, тобто стандартам архітектури відкритих систем, називають відкритими, а системи, що не відповідають цим вимогам, вважаються закритими. У моделі ВВС визначено сім рівнів.

Модель фізичної реалізації показує, які функції в якій апаратурі втілено, а також за допомогою яких протоколів реалізовуються логічні інтерфейси між різними апаратними засобами.

Така модель є основою взаємодії оператора мережі й постачальників обладнання і ПЗ. Вона також дозволяє визначити додаткові інтерфейси між обладнанням від різних постачальників та їхні характеристики, що підлягають стандартизації.

1.2. Еталонна модель взаємодії відкритих систем

1.2.1. Характеристика та призначення рівневих протоколів

Обслуговування користувача – це реалізація визначеного набору функцій, що належать до передачі даних і зв'язані з такими елементами:

- мовою (включаються і функції перетворення форматів, трансляції і редагування);
- дисципліною діалогу для керування потоком даних (наприклад, послідовністю роботи, чеканням відповіді);
- керуванням передачею даних, у тому числі керуванням швидкістю передавання даних з урахуванням наявності засобів обробки потоків даних в абонента на обох кінцях лінії і керуванням послідовністю передавання для забезпечення вірогідності даних, що передаються;
- транспортуванням даних (включається проходження сигналів по більш-менш складній мережі між пристроями, кожен з яких має деяку адресу в мережі).

Групові діалоги або сесії можуть здійснюватися паралельно між будь-яким одним елементом та іншими елементами. Для забезпечення керованого використання мережі необхідне введення послуг для користувача з боку мережі. Щоб обслуговувати мережу і керувати нею, потрібні й інші служби мережі, звичайно недоступні і невідомі користувачеві.

Мережна архітектура систем регламентує набір функцій передачі даних, що розподілені по всій мережі, вона також визначає формати і протоколи, які зв'язують ці розподілені функції між собою. Мета створення мережної архітектури полягає в досягненні надійної передачі даних між програмами, операторами, операторами й запам'ятовуючими пристроями, розташованими в будь-якому пункті мережі. Проте з цього не витікає, що всі функції, які виконуються мережею, повністю регламентуються її архітектурою. Доцільніше, щоб деякі функції і (або) адаптери створювалися розробниками апаратури або замовниками. У рамках архітектури в першу

чергу уніфікуються ключові формати і протоколи, які потрібні для забезпечення передачі даних.

Архітектура зв'язку в розподілених системах створювалася в два етапи. На першому були розроблені однорідні мережні архітектури, призначені для застосування однотипного устаткування. Наприклад, мережна архітектура SNA (System Network Architecture), створена фірмою IBM, була покладена в основу однієї з перших глобальних обчислювальних мереж CLLIA. На другому етапі за основу прийнято базову еталонну модель ВВС (взаємодії відкритих систем), що була першим стандартом, розробленим Міжнародною організацією стандартизації.

Концепції мережних протоколів розвивалися протягом останніх двадцяти років і були спрямовані на забезпечення:

– логічної декомпозиції складної мережі на менші, зрозуміліші частини (рівні); стандартних інтерфейсів між мережними функціями, наприклад стандартних інтерфейсів між модулями програмного забезпечення;

– симетрії стосовно функцій, реалізованих у кожному вузлі мережі. Кожний рівень у деякому вузлі мережі виконує ті ж самі функції, що й аналогічний рівень в іншому вузлі:

– забезпечує засоби передбачення змін і керування змінами, які можуть бути внесені в мережну логіку (програмне забезпечення або мікропрограми);

– реалізує просту стандартну мову комунікації розробників мереж, адміністраторів, фірм-постачальників і користувачів, використовувану під час обговорення мережних функцій.

Можна зробити висновок, що загальна проблема зв'язку, яка полягає в забезпеченні своєчасної, правильної та розпізнаваної доставки даних кінцевому користувачеві, зайнятому в сеансі зв'язку в мережі або в декількох мережах, поділяється на дві частини. Перша стосується мережі зв'язку: дані, що передаються кінцевому користувачеві з мережі, повинні надійти за призначенням в правильному вигляді та своєчасно. Друга частина проблеми – дані, що надійшли зрештою за призначенням кінцевому користувачеві, повинні розпізнаватись і мати належну форму для їх правильного використання, – можна вирішити введенням протоколів високого рівня. Повна архітектура, орієнтована на кінцевого користувача, містить у собі і мережні протоколи і протоколи високого рівня. Як приклад, на рисунку 1.4 показано схему зв'язку між користувачами А і В через проміжний вузол мережі. До цього вузла можуть бути приєднані кінцеві користувачі, а з ними можуть бути зв'язані протоколи високого рівня, але функцією проміжного вузла є тільки надання відповідних мережних послуг.

У свою чергу, дві групи протоколів – ті, що надають мережні послуги, і протоколи високого рівня – звичайно поділяються далі на окремі рівні. Кожний рівень вибирається для надання визначеної послуги за змістом названих основних завдань: правильністю і своєчасністю доставлення даних у формі, за якою їх можна розпізнати. Шляхом розробки еталонної моделі

взаємодії відкритих систем була побудована концепція, при якій кожний рівень надає послуги вищестоящому рівню.

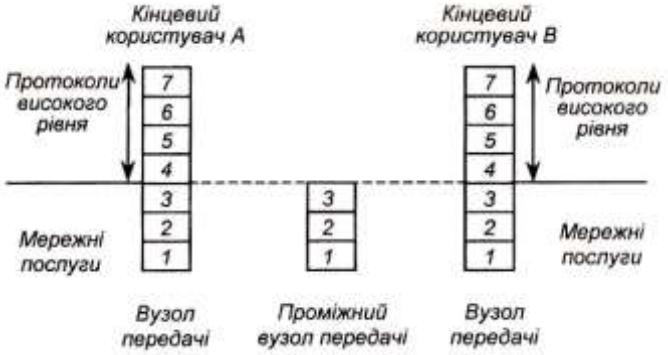


Рисунок 1.4 – Архітектура багаторівневого зв’язку

1.2.2. Рівні еталонної моделі взаємодії відкритих систем

Модель рівневих протоколів взаємодії відкритих систем є семирівневим стандартом. Рівні в мережній моделі, запропонованій ISO, наведено на рисунку 1.5.

Міжнародною організацією стандартизації розроблено базову еталонну модель ВВС для визначення рівневих мереж і рівневих протоколів. Ця модель привернула велику увагу в усьому світі і була реалізована багатьма фірмами – виробниками засобів зв’язку.

Метою моделі ВВС є: стандартизація обміну даними між системами; усунення будь-яких технічних перешкод для зв’язку систем; усунення труднощів "внутрішнього" опису функціонування окремої системи; визначення точок взаємосполучення для обміну інформацією між системами; звуження діапазону можливостей послуг для того, щоб підвищити здатність обміну даними між користувачами без зайвих накладних витрат на переговори і переклад; забезпечення розумної відправної точки відходу від стандартів, якщо вони не задовольняють усіх вимог.

Найнижчий рівень називається фізичним. Функції цього рівня забезпечують активізацію, підтримку і деактивізацію фізичного ланцюга між кінцевим устаткуванням даних (КУД) і апаратурою каналу даних (АКД). Для фізичного рівня опубліковано велику кількість стандартів. Найбільш відомими є RS-232C і рекомендації МСЕ.

Канальний рівень (рівень ланки даних) відповідає за передачу даних по каналу. Він забезпечує: синхронізацію даних для розмежування потоку бітів фізичного рівня; вид подання бітів; визначені гарантії прибуття даних в приймальне КУД; керування потоком даних, щоб КУД не перевантажувалися в будь-який момент часу занадто великою кількістю даних.

Одна з найважливіших функцій цього рівня полягає у виявленні помилок передачі і забезпеченні механізму відновлення даних у випадку їх втрати, дублювання за наявності помилок у даних.

Мережний рівень визначає інтерфейс КУД користувача з мережею пакетної комутації, інтерфейс двох пристроїв КУД один з одним у мережі

пакетної комутації, а також маршрутизацію в мережі і зв'язок між мережами (інтермережний протокол). Цей рівень детально визначений і має велику кількість функцій. Протокол X.25 реалізує цей рівень.

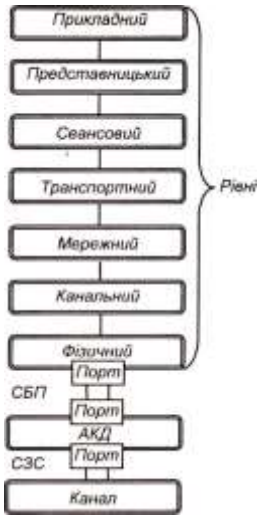


Рисунок 1.5 – Рівні в мережній моделі, запропонованій ISO:
СБП – стик блока приєднання; СЗС – стик, що залежить від середовища

Транспортний рівень забезпечує інтерфейс між мережею передачі даних і верхніми трьома рівнями. Саме цей рівень надає користувачеві факультативні можливості одержання сервісу визначеної якості (і вартості) від самої мережі (тобто мережного рівня). Він проектується таким чином, щоб відокремити користувача від деяких фізичних і функціональних аспектів пакетної мережі, а також забезпечує наскрізну звітність у мережі.

Сеансовий рівень служить інтерфейсом користувача з рівнем транспортних послуг. Цей рівень забезпечує засоби організації обміну даними між користувачами. **Користувачі можуть вибрати тип синхронізації і керування, що вимагаються від рівня, такі як:**

– почергово або одночасно двоспрямований діалог;
– точки синхронізації для проміжного контролю і відновлення при передачі файлів;
– аварійне закінчення і рестартування;
– нормальна і прискорена передача даних.

Сеансовий рівень має спеціальні послуги, примітивні і протокольні блоки даних, що визначені в документах ISO і МСЕ.

Представницький рівень даних визначає синтаксис даних у моделі. Він не пов'язаний зі значенням або семантикою даних. Його головна роль полягає в тому, щоб приймати типи даних (знак, ціле число) з прикладного рівня і потім узгоджувати з рівнем того ж рангу синтаксичне подання (таке, як телетекс, відеотекс і т. д.). Рівень подання забезпечує відображення даних на віртуальному терміналі, а також надання таких послуг, як дозвіл прийому електронного повідомлення від рівня додаткових програмних продуктів і узгодження з одноранговим рівнем виду подання сторінки (наприклад, для друкарського набору), для прикладного рівня іншого вузла користувача.

Прикладний рівень призначений для підтримки прикладного процесу кінцевого користувача. На відміну від рівня подання даних цей рівень має справу із семантикою даних. Рівень містить сервісні елементи для підтримки прикладних процесів, таких як керування різноманітними процесами, обмін фінансовими даними, діловими і довідковими даними (наприклад, система обробки повідомлень). Прикладний рівень також підтримує концепції віртуального терміналу і віртуального файлу.

1.2.3. Структура повідомлення за моделлю ВВС

Багаторівнева організація керування процесами в мережі породжує необхідність модифікувати на кожному рівні повідомлення стосовно функцій, реалізованих на цьому рівні. Модифікація виконується за схемою взаємодії процесів, поданою на рисунку 1.6. Даним, що передаються у формі повідомлення, надаються заголовок і закінчення, в яких міститься інформація, необхідна для опрацювання повідомлення на відповідному рівні: покажчики типу повідомлення, адреси відправника, одержувача, каналу, порту і т.д.

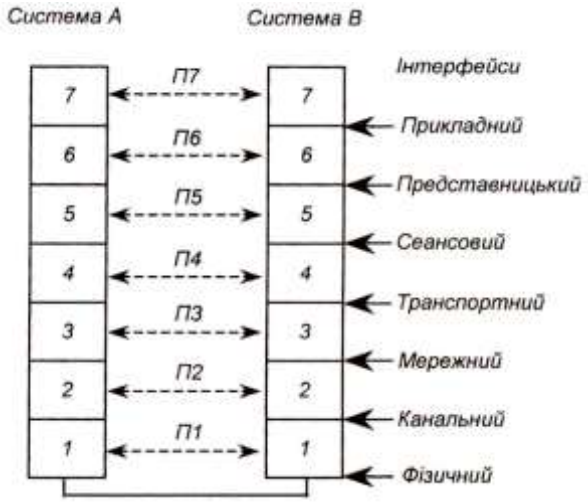


Рисунок 1.6 – Схема взаємодії процесів на базі домережних протоколів і інтерфейсів

Заголовок і закінчення називаються обрамленням повідомлення (даних). Повідомлення, сформоване на рівні n+1, при обробці на рівні n супроводжується додатковою інформацією у вигляді заголовка $З_n$ і закінчення $К_n$. Це ж повідомлення, надходячи на нижчий рівень, у черговий раз забезпечується додатковою інформацією – заголовком $З_{n-1}$ і закінченням $К_{n-1}$. У разі передавання від нижчих рівнів до вищих повідомлення звільняється від відповідного обрамлення. Таким чином, кожний рівень оперує власними заголовком і закінченням, а послідовність символів, що знаходиться між ними, розглядається як дані більш високого рівня. За рахунок цього забезпечується незалежність даних, що стосуються різних рівнів керування передачею повідомлень.

Пояснимо цей процес. Супроводження повідомлені, обрамленням – процедура, аналогічна вкладанню листа в конверт, який використовується у поштовому зв'язку. Всі дані, необхідні для передачі повідомлення, вказуються на конверті. При передачі цього повідомлення на нижчий рівень воно вкладається в новий конверт, забезпечений відповідними даними. Повідомлення, що надходить у систему, проходить від нижніх рівнів до верхнього (дивись рисунок 1.6). Засіб керування нижнього рівня оперує даними, зазначеними в обрамленні, як і з даними на конверті. При передаванні на вищий рівень повідомлення звільняється від "конверта", внаслідок чого на наступному рівні обробляється черговий "конверт". Таким чином, кожний рівень керування оперує не з самими повідомленнями, а з "конвертами", в які "упаковані" повідомлення. Тому склад повідомлень, що формуються на верхніх рівнях, ніяк не впливає на функціонування нижніх рівнів керування передачею. Процес передавання повідомлення відбувається послідовно з 7-го рівня на 1-й, а процес прийому – з 1-го на 7-й.

1.2.4. Протоколи в ТІМ та зв'язок між рівнями

Обмін повідомленнями (даними) допускається тільки між процесами одного рівня. Це означає, що прикладний процес може взаємодіяти тільки з прикладним процесом, а процеси керування передавання повідомлень на рівнях 1, 2,... – тільки з процесами однойменних рівнів. Ця схема взаємодії процесів (рисунок 1.6), як і процедура обрамлення повідомлень, – необхідна умова логічної незалежності рівнів інформаційних мереж.

Прикладний процес у системі А (рівень 7) формує повідомлення прикладного процесу в системі В, пристосовуючись тільки до логіки взаємодії цих двох прикладних процесів, але не до організації мережі. Фактично повідомлення, сформовані процесом у системі А, проходять послідовно через рівні 6, 5,..., 1, зазнаючи процедури послідовного обрамлення, передаються по каналу зв'язку, і потім через рівні 1, 2,..., 6, на яких з повідомлень послідовно знімається обрамлення, надходять до процесу в системі В повністю розконвертованими. Аналогічно процес керування транспортуванням повідомлень у базову мережу (рівень 4) відправляє власні дані в обрамленні-повідомлення. Всі дані, що знаходяться поза обрамленням, не мають ніякого значення для цього процесу. Таким чином, процеси одного рівня в різних системах обмінюються даними в основному за допомогою заголовків і закінчень повідомлень. Системний процес може послати власне повідомлення іншому процесу такого ж рівня у встановленому порядку. При цьому весь текст повідомлення буде належати однойменному процесові в іншій системі. Такі повідомлення називаються керуючими і використовуються в основному на рівнях 2-5.

Процедура взаємодії процесів однойменних рівнів двох різних систем на основі обміну повідомленнями (даними) називається протоколом. Для процесів кожного рівня використовуються протоколи П1, П2,..., П7.

Процедура взаємодії різних рівнів в одній системі називається інтерфейсом.

Описуючи протокол, прийнято виділяти його логічну і процедурну характеристики. Логічна характеристика протоколу – структура (формат) і зміст (семантика) повідомлень. Логічна характеристика задається переліком типів повідомлень та їх змістом. Правила виконання дій, запропонованих протоколом взаємодії, називаються процедурною характеристикою протоколу. Ця характеристика може зображуватися в різній математичній формі: операторними схемами алгоритмів, автоматними моделями, мережами Петрі та ін.

Логіка організації інформаційної мережі найбільшою мірою визначається протоколами, що встановлюють як тип і структуру повідомлень, так і процедури їх обробки – реакцію на вхідні повідомлення і генерацію власних повідомлень. Число рівнів керування і типи використовуваних протоколів багато в чому визначають архітектуру мережі.

Як було відзначено вище, кожний рівень є постачальником сервісу і може складатися з декількох сервісних функцій. Наприклад, один із рівнів може забезпечувати сервісні функції за кодовими перетвореннями.

Функція – це деяка підсистема рівня (деяка реальна підпрограма в якійсь програмі). Кожна підсистема може, складатися з логічних об’єктів – деяких спеціалізованих модулів.

Основна ідея обміну між вузлами полягає в тому, що на кожному рівні додаються послуги цього рівня до послуг, які забезпечуються нижніми рівнями. Отже, верхній рівень, що взаємодіє безпосередньо з додатковим програмним продуктом кінцевого користувача, має повний набір послуг усіх нижніх рівнів. Верхні рівні диктують нижнім, які послуги мають бути викликані.

1.2.5. Розподіл мережного обладнання за моделлю ВВС

Інформаційну мережу за характером взаємодії відкритих систем можна подати у вигляді трьох типів систем: абонентські, адміністративні й асоціативні.

Абонентські системи призначені для обробки прикладних процесів користувачів, тому в області взаємодії вони ніби розсікаються на сім рівнів і на базі комунікаційної підмережі мають структуру, показану на рис. 5. Паралельно в системі реалізується ієрархія протоколів, що підтримує прикладні процеси керування мережею. Ці протоколи можуть бути такими ж, як і в ієрархії, що підтримує прикладні процеси користувачів, але можуть і відрізнятися від них. Усі рівні в системі зв’язані процесом керування системою.

Якщо є така можливість, то слід звільнити користувальницьку ЕОМ абонентської системи від виконання функцій області взаємодії, щоб надати їй можливість ефективно виконувати прикладні процеси. З цією метою абонентську систему поділяють на дві частини (рисунок 1.7): термінальне

обладнання і станцію. Термінальне обладнання є основною частиною системи, що виконує прикладні процеси і, якщо є потреба, то і протоколи верхніх рівнів. Станція – допоміжна частина системи, вона реалізує протоколи нижніх або всіх рівнів. За кількістю протоколів, що реалізуються, станцію називають канальною, транспортною або абонентською.

Канальна станція виконує протоколи 1 і 2, транспортна – протоколи 1…4. Абонентська станція реалізує всі сім рівнів області взаємодії відкритих систем.

Рисунок 1.7 – Структура абонентської й адміністративної систем

Станція й термінальне обладнання з'єднуються каналом або шиною. В обох випадках це з'єднання має бути подано спеціальним фізичним (1) і канальним (2) протоколами. Перший з них визначає характеристики каналу (шини), а другий описує процедури керування каналом (шиною) і передавання ними блоків даних. Спеціальні протоколи (1', 2') не є стандартними ISO (ВВС). Вони залежать від конкретних обраних каналів (шин), методів зв'язку зі станціями.

Канальна станція (рисунок 1.8) є найпростішою, тому що реалізує лише протоколи двох рівнів (1, 2) взаємодії.

Рисунок 1.8 – Поділ абонентської системи на термінальне обладнання та станцію

Проте ця простота вимагає значного завантаження абонента, який має виконувати функції, що описуються протоколами інших п’яти рівнів.

Ефективною є абонентська станція, яка цілком розвантажує термінальне обладнання від виконання функцій, що забезпечують взаємодію в мережі прикладних процесів. Проте в складному термінальному обладнанні часто працюють кілька комплексів прикладних процесів. Обмін же інформацією між ними відбувається через сеансовий рівень. Тому в тих випадках, коли рівень 5 знаходиться в станції, робота термінального обладнання залежить від надійності, завадостійкості та пропускної спроможності каналу (шини) і станції, що є не завжди прийнятним.

Тому найчастіше використовується транспортна станція. Вона виконує всі функції, пов’язані з передаванням інформації між комплексами термінального обладнання через усю комунікаційну підмережу. Що стосується термінального обладнання, то воно забезпечує виконання прикладних процесів, які підтримуються прикладним, представницьким і сеансовим протоколами.

Абонентські системи є основними компонентами інформаційної мережі. Ці системи будуються на основі різноманітних ЕОМ, що виготовляються виробниками різних країн. Тому для кожного типу комутаційної підмережі розробляється абонентський інтерфейс (рисунок 1.8), що визначає параметри і процедури взаємодії всіх абонентських систем із комунікаційною підмережею.

Адміністративна система має ту ж структуру, що й абонентські (рисунок 1.7 та рисунок 1.8), але замість прикладних процесів користувачів виконуються прикладні процеси керування мережею або її частиною.

Асоціативна система на відміну від абонентської й адміністративної не здійснює обробки інформації для потреб користувачів і керування мережею. Вона призначена для з’єднання в одне ціле частин інформаційних мереж і забезпечення взаємодії цих мереж між собою.

За характеристиками об’єднуваних частин мереж і різних мереж розрізняють чотири типи асоціативних систем (рисунок 1.9). Найскладнішою з них є шлюз. Він забезпечує взаємодію двох або більше інформаційних мереж із різними наборами протоколів семи рівнів. Так, на рисунку 1.9 показано два набори: 1′-7′ і 1"-7", зв’язані спеціальними прикладними процесами. Ці процеси перетворюють один семирівневий набір протоколів в інший, забезпечуючи необхідну взаємодію.

Слід зазначити, що шлюзи найчастіше використовуються в тих випадках, коли потрібно об’єднати інформаційні мережі, створені за різними фірмовими стандартами. Коли ж проектується група мереж відповідно до стандартів ВВС, доцільним є інший підхід: в мережах, що з’єднуються, протоколи рівнів 4…7 слід реалізовувати однаковими. Це дозволяє для з’єднання мереж використовувати не шлюзи, а більш асоціативні системи – маршрутизатори та мости.

Функція маршрутизатора – забезпечення взаємодії комунікаційних підмереж. Останні характеризуються лише трьома рівнями протоколів. Тому

логічна структура маршрутизатора має вигляд, показаний на рисунок 1.9. Як бачимо, маршрутизатор не має протоколів рівнів 4…7 і є прозорим для них. Його завданням є перетворення протоколів трьох нижніх рівнів. Іноді в інформаційних мережах маршрутизатори зв'язують частини комунікаційної підмережі, в яких використовуються однакові протоколи рівнів 1…3. Такі маршрутизатори мають назву вузлів комутації пакетів. Перетворення протоколів у них не виконується: мережні процеси здійснюють лише комутацію і маршрутизацію інформації. У з'єднуваних вузлами підмережах має здійснюватися загальна адресація абонентських систем.

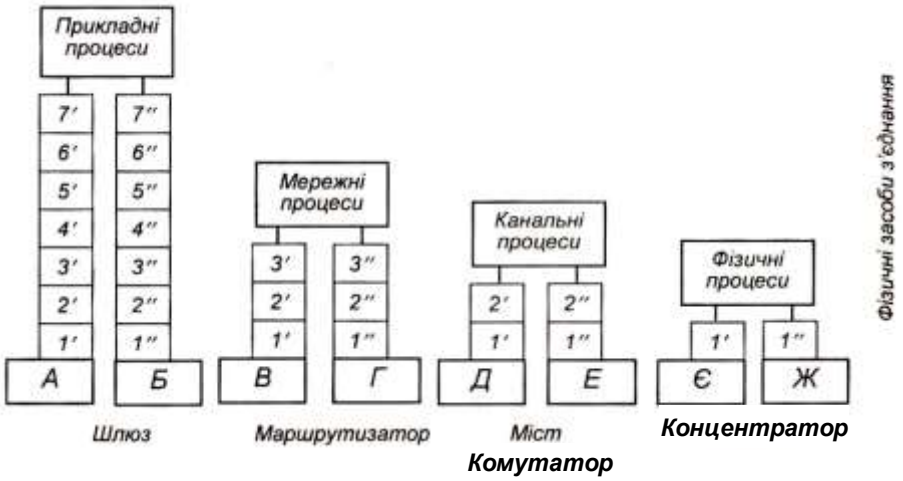


Рисунок 1.9 – Типи асоціативних систем

Мости (рисунок 1.9) призначені для з'єднання частин мереж, різноманітних типів каналів передачі даних. Будь-який канал визначається протоколами рівнів 1 і 2, тому логічна структура моста має дворівневу структуру. Канальні процеси в даному випадку перетворюють протоколи обох рівнів. У разі використання мостів у з'єднуваних підмережах мають бути погоджені структура адреси і розмір кадрів.

Більш складні, або інтелектуальні мости, крім зазначених функцій, виконують також роль фільтрів, що не пропускають пакети, не адресовані іншій частині мережі.

У кожному інтелектуальному мості міститься невеличка база даних, до якої вносяться адреси систем обох підмереж, контрольна сума, призначена для перевірки кадру, що використовується не тільки на вході моста, але й на його виході. Це дозволяє запобігати появі помилок усередині моста. Завдяки простоті виконуваних функцій застосовуються мости з відносно нескладною структурою, вони працюють з високою швидкістю. Формати блоків даних, що передаються, і розміри цих блоків міст не змінює.

Отже, асоціативні системи реалізують міжмережні, мережні, канальні та фізичні процеси. Вони виконують функції, у тому числі й перетворення, потрібні для з'єднання частин мереж або цілих мереж.

Об'єднання мереж здійснюється установленням з'єднання або без нього. Об'єднання з установленням з'єднання дає змогу заздалегідь

розподіляти буфери та інші ресурси системи. У цьому випадку забезпечується просте і надійне керування потоками інформації, що проходять з однієї мережі в іншу, а також здійснюються повідомлення про втрату блоків даних і упорядкування послідовностей цих блоків. Проте організація і підтримка міжмережних з'єднань потребує виконання складних протоколів.

Об'єднання мереж без установлення між ними з'єднань характеризується простотою протоколів і високою швидкістю роботи асоціативної системи. Проте цей спосіб не має тих переваг, які притаманні об'єднанням з установленням з'єднання. Тому для забезпечення якісного передавання інформації абонентські системи обох мереж повинні мати потужні версії транспортних протоколів.

Відповідно до наведеного вище при об'єднанні мереж використовуються дві моделі. Перша з них, протокольна, характеризується тим, що у верхній частині мережного рівня розташовується міжмережний протокол. Завдяки його наявності обидві об'єднуючі мережі можуть працювати практично як одна загальна мережа. У цьому випадку асоціативна система забезпечує комутацію інформації, що проходить через систему. Другою моделлю об'єднання мереж є естафетна. У такій моделі міжмережний протокол практично відсутній і передавання керуючої інформації через асоціативну систему не відбувається. Внаслідок цього в кожній мережі повинно проводитися розпізнавання глобальних адрес, на основі якого вибираються маршрути передавання інформації.

Контрольні питання до розділу 1

1. Наведіть та охарактеризуйте основні вимоги до зв'язку.
2. Опишіть порядок роботи сеансового рівня моделі ВВС (OSI).
3. Наведіть схему інформаційної мережі. Поясніть призначення складових.
4. Охарактеризуйте основні схеми реалізації структурної будови мереж (КЕС, РЕС і т.ін.)
5. Наведіть та опишіть рівні еталонної моделі ВВС (OSI).

РОЗДІЛ 2
ОСНОВНІ ХАРАКТЕРИСТИКИ, АНАЛІЗ І СИНТЕЗ ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖ

2.1. Основні характеристики телекомунікаційних мереж

2.1.1. Класифікація мереж

Для класифікації мереж передачі даних використовуються різні ознаки:

1. За розміром охопленої території:

Локальна мережа (LAN, Local Area Network) Локальна обчислювальна мережа (ЛОМ) – мережа передачі даних (рисунок 2.1), що покриває зазвичай відносно невелику територію або невелику групу будівель (будинок, офіс, фірму, інститут).

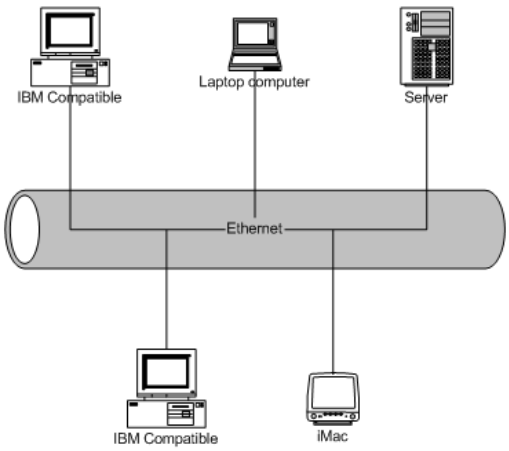


Рисунок 2.1 – Локальна обчислювальна мережа

Глобальна обчислювальна мережа, ГОМ (англ. Wide Area Network, WAN) є мережею передачі даних, що охоплює великі території і що включає десятки і сотні тисяч комп'ютерів. ГОМ служать для об'єднання розрізнених мереж так, щоб користувачі і комп'ютери, де б вони не знаходилися, могли взаємодіяти з усіма іншими учасниками глобальної мережі (рисунок 2.2). Деякі ГОМ побудовані виключно для приватних організацій, інші є засобом комунікації корпоративних ЛОМ з глобальною мережею Інтернет або за допомогою Інтернет з видаленими мережами, що входять до складу корпоративних. Частіше усього ГОМ спирається на виділені лінії, на одному кінці яких маршрутизатор підключається до ЛОМ, а на іншому концентратор зв'язується з іншими частинами ГОМ.

Глобальні мережі відрізняються від локальних тим, що розраховані на необмежене число абонентів і використовують, як правило, не надто якісні канали зв'язку. Правда, зараз вже не можна провести чітку і однозначну межу між локальними і глобальними мережами. Більшість локальних мереж

мають вихід в глобальну мережу, але характер переданої інформації, принципи організації обміну, режими доступу, до ресурсів усередині локальної мережі, як правило, сильно відрізняються від тих, що прийнято в глобальній мережі. І хоча усі комп'ютери локальної мережі в даному випадку включені також і в глобальну мережу, специфіку локальної мережі це не відміняє. Можливість виходу в глобальну мережу залишається усього лише одним з ресурсів, поділені користувачами локальної мережі. Більш того останнім часом відокремлюють поняття міських обчислювальних мереж (MOM) (з англійської Metropolitan – місто, мегаполіс, Metropolitan Area Network, MAN) – мережі масштабу міста, великого регіону, які займають проміжне місце між мережами LAN та WAN.

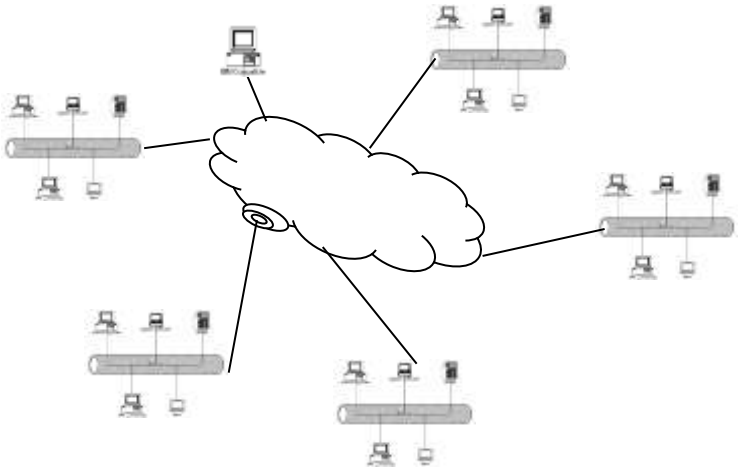


Рисунок 2.2 – Глобальна обчислювальна мережа

2. За типом функціональної взаємодії

Однорангова архітектура (peer-to-peer architecture) – це концепція мережі, в якій її ресурси розосереджені по усіх системах (рисунок 2.3). Ця архітектура характеризується тим, що в ній усі системи рівноправні.

До однорангових мереж відносяться малі мережі, де будь-яка робоча станція може виконувати одночасно функції файлового сервера і робочої станції.

Рисунок 2.3 – Однорангова архітектура

Мережа на основі сервера (рисунок 2.4). Така мережа характеризується наявністю одного особливого комп'ютера (сервера) та низькі інших (робочих

станцій). **Сервер** – це об’єкт, що надає сервіс іншим об’єктам мережі по їх запитах (сервіс – це процес обслуговування клієнтів). На сервері зосереджена переважна більшість ресурсів мережі.

Рисунок 2.4 – Архітектура клієнт-сервер

Віртуальна приватна мережа (VPN – Virtual Private Network) – представляє собою об’єднання кількох окремих комп’ютерів або локальних мереж у віртуальну мережу, яка забезпечує обертання інформації між ними у захищеному режимі навіть при використанні громадської телекомунікаційної інфраструктури (рисунок 2.5). Це досягається шляхом застосування шифрування даних, перевірки їх цілісності та тунелювання (дані однієї мережі передаються через іншу мережу або через безпечний доступ до своєї мережі).

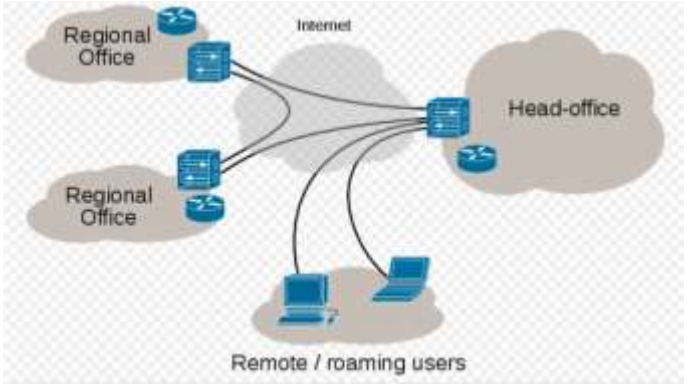


Рисунок 2.5 – Віртуальна приватна мережа (VPN)

3. За типом мережної топології.

Під топологією мережі розуміється опис її фізичного розташування, тобто те, як комп’ютери сполучені в мережі один з одним і за допомогою яких пристроїв входять у фізичну топологію.

Існує чотири основні топології:

- Bus (шина);
- Ring (кільце);
- Star (зірка);
- Mesh (осередок).

2.1.2. Якість обслуговування в телекомунікаційних мережах

Якість послуг телекомунікацій характеризується сукупністю наступних основних споживчих властивостей: забезпеченістю, зручністю використання, дієвістю, безпекою й іншими властивості, специфічними для кожної послуги.

Забезпеченість послуги – здатність оператора зв'язку надавати послугу (набір послуг) і забезпечувати обслуговування користувача щонайкраще.

Зручність використання – властивість послуги, що характеризує, наскільки успішно й просто користувач може її одержати

Дієвість – властивість послуги бути наданої тоді, коли це необхідно користувачеві, і тривати без надмірного погіршення протягом необхідного часу (у межах певних допусків і в заданих умовах).

Безпека – властивість послуги бути захищеної від несанкціонованого доступу, зловмисного й неправильного використання, навмисного псування, помилок людини й стихійних лих.

Із чотирьох перерахованих вище властивостей найважливішим є ***дієвість***, яка, у свою чергу, має три складові:

- **доступність** – властивість послуги бути наданої тоді, коли це необхідно користувачеві;
- **безперервність** – властивість послуги, будучи наданої, тривати протягом необхідного часу;
- **цілісність** – властивість послуги, будучи наданої, забезпечуватися без надмірного погіршення.

Існуюче різноманіття різних визначень характеризує складність визначення всіх аспектів, що ставляться до поняття QoS. У Рекомендації МСЭ-Т E.800 [4] дане наступне визначення QoS: "сукупний показник експлуатаційних характеристик послуги, що визначає ступінь задоволеності користувача послугою".

З одного боку якість послуг залежить від характеристик функціонування мережі. Характеристики функціонування мережі визначають здатність мережі або її частини виконувати функції, що забезпечують передачу інформації між користувачами. З іншого боку QoS – це результат сприйняття користувача або експлуатаційні характеристики мережі в цілому. Таким чином, QoS не тільки задається або визначається показниками, які можуть бути виражені технічними показниками, але також визначається суб'єктивним показником, який визначає очікуване й сприймане користувачем якість.

Параметри якості послуги – значення, отримані в результаті вимірів і/або опитувань користувачів, що оцінюють показники якості послуг.

Отже показники якості послуг зв'язку розділяються на технічні показники й показники задоволеності абонентів і користувачів послугами й наведено в таблиці 2.1 і таблиці 2.2 відповідно.

Таблиця 2.1 – Технічні показники якості послуг зв’язку

Основні послуги	**Найменування показника якості послуги, одиниця виміру**	**Визначення**
Послуга фіксованого телефонного зв’язку	Частка неуспішних викликів при встановленні з’єднань через відмову мережі зв’язку, %	Відношення числа неуспішних спроб установлення з’єднань із викликуваним абонентом до загального числа спроб установлення з’єднань, виражене у відсотках $p_{\text{в}} = \frac{N_{\text{н}}}{N} 100$
	Середній час установлення телефонного з’єднання: місцевого, внутрішньозонового, міжміського, с.	Час від набору останньої цифри телефонного номера до одержання кінцевим устаткуванням інформації про відповідь від кінцевого встаткування викликуваного абонента, $t_{\text{вс.сер}}$
	Середня бальна оцінка якості передачі мови по п’ятибальній шкалі, од.	Середня бальна оцінка якості передачі мови при об’єктивному методі оцінки визначається за допомогою приладу, при проведенні статистичних випробувань
	Частка успішно переданих факсимільних повідомлень, %	Відношення числа успішних спроб передачі факсимільних повідомлень до загального числа спроб передачі факсимільних повідомлень, виражене у відсотках $q_{\text{п}} = \frac{N_{\text{у}}}{N} 100$
Послуга доступу в мережу Інтернет (фіксований і мобільний)	Середній час авторизації користувача в мережі Інтернет, с	Час від моменту завершення введення логіна й пароля до моменту підключення до мережі зв’язку, $t_{\text{ав.сер}}$
	Мінімальна й середня швидкості передачі, кбіт/с	Швидкість передачі в напрямку від/ до абонента до/від мережі зв’язку $B_{\text{пер(пр).сер(min)}}$
	Середня затримка передачі пакетів інформації, мс	Половина середнього часу з моменту передачі кінцевим устаткуванням запиту до сервера до моменту одержання кінцевим устаткуванням відповіді від сервера $t_{\text{з.сер}} = \frac{t_{\text{відп}}}{2}$
	Середнє відхилення затримки передачі пакетів, мс	Середнє відхилення від середнього значення затримки передачі пакетів $\Delta t_{\text{з.сер}}$
	Частка неуспішних спроб передачі інформації (передачі тестових файлів), %	Відношення числа спроб неуспішної передачі інформації (тестових файлів) до загального числа спроб передачі інформації за певний період часу, виражене у відсотках $p_{\text{н}} = \frac{N_{\text{н}}}{N} 100$

Основні послуги	Найменування показника якості послуги, одиниця виміру	Визначення
	Частка успішних спроб доступу до мережі Інтернет, %	Відношення числа успішних спроб доступу до мережі Інтернет до загального числа спроб доступу до мережі Інтернет за умови, коли мережа зв'язки перебуває в стані готовності, виражене у відсотках $q_д = \frac{N_у}{N} 100$
Послуги рухомого радіотелефонного зв'язку	Частка неуспішних викликів при встановленні з'єднань у мережі рухомого зв'язку, %	Відношення числа неуспішних спроб установлення з'єднань із викликуваним абонентом до загального числа спроб установлення з'єднань, отриманих за результатами вимірів на мережі, проведених у різні періоди протягом року (календарного й/поточного), виражене у відсотках
	Середній час установлення телефонного з'єднання в мережі рухомого зв'язку, с.	Час від набору останньої цифри телефонного номера абонента викликуваного до одержання кінцевим устаткуванням зухвалого абонента інформації про відповідь від кінцевого встаткування викликуваного абонента
	Середня бальна оцінка якості передачі мови по п'ятибальній шкалі, од.	Середня бальна оцінка якості передачі мови при об'єктивному методі оцінки визначається за допомогою приладу, що реалізує алгоритм визначення середньої абонентської оцінки відповідно до міжнародних рекомендацій, шляхом усереднення оцінок, отриманих по кожному встановленому з'єднанню при проведенні статистичних випробувань
	Покриття мережі, %	Здатність мережі надавати послуги зв'язку на вимогу користувача
	Коефіцієнт успішно переданих SMS	Часовий інтервал від моменту передачі відправником короткого повідомлення в центр обслуговування коротких повідомлень до моменту одержання від центру підтвердження про приймання SMS
	Час доставки SMS	Часовий інтервал (у секундах) від моменту передачі відправником короткого повідомлення в SMSC до моменту його одержання абонентським терміналом одержувача

Основні послуги	Найменування показника якості послуги, одиниця виміру	Визначення
Універсальні послуги зв’язку, включаючи:		
– послуги телефонного зв’язку з використанням таксофонів;	Частка таксофонів у робочому стані, %	Відношення числа робочих таксофонів до загального числа таксофонів, зафіксованих на мережі оператора зв’язки, виражене у відсотках
– послуги з передачі даних і наданню доступу до мережі "Інтернет"	Швидкість доступу, кбіт/с	

Таблиця 2.2 – Показники задоволеності абонентів і користувачів послугами зв’язку

№ п/п	Показники якості, одиниця виміру	Визначення
1.	Своєчасність виконання заявки на підключення клієнта до мережі зв’язку, включаючи доступ до мережі Інтернет, %	Відношення числа заявок на підключення клієнтів до мережі зв’язку, виконаних у встановлений термін до загального числа заявок, виражене у відсотках
2.	Середній час перевищення встановленого строку виконання заявки на підключення клієнта до мережі зв’язку, включаючи доступ до мережі Інтернет, днів	Середня кількість днів затримки виконання заявок стосовно встановленого строку
3.	Своєчасність надання послуги з переносу абонентського номера, %	Відношення числа заявок на перенос абонентського номера з перевищенням установленого строку переносу номера до загального числа заявок на перенос абонентського номера, виражене у відсотках
4.	Кількість пошкоджень розраховуючи на одну абонентську лінію в рік, одиниць	Відношення числа обґрунтованих записів про несправності, зафіксовані службами експлуатації мережі за рік (календарних і/або поточних), до середнього числа абонентських ліній, зафіксованих протягом року
5.	Частка пошкоджень, усунутих у контрольний термін, %	Відношення кількості несправностей, зафіксованих по заявах абонентів і усунутих за час, рівне (або менше) часу, установленому контрольними строками, до загального числа обґрунтованих несправностей на кінець року (календарного й/або поточного)

№ п/п	Показники якості, одиниця виміру	Визначення
6.	Доступність служби оператора, с	Час відповіді служби оператора
		Час відповіді фахівця служби
7.	Правильність рахунків, що виставляються за послуги зв'язку, %	Відношення числа правильно виставлених рахунків на послуги зв'язку до загальної кількості виставлених рахунків, виражене у відсотках
8.	Претензії на помилки в рахунках по заздалегідь оплаченому кредиту, %	Відношення числа претензій, пов'язаних з помилками в рахунках по заздалегідь оплаченому кредиту, до загального числа рахунків по заздалегідь оплаченому кредиту, виражене у відсотках
9.	Число претензій на один абонента, од.	Відношення загального числа претензій, на кінець року (календарного й/або поточного) до абонентів
10.	Число претензій, задоволених у встановлений термін, %	Відношення числа претензій, задоволених у встановлений термін до загального числа претензій, виражене у відсотках
11.	Частка повторних звернень користувача в служби оператора зв'язку, %	Відношення числа повторних звернень користувачів до загального числа звернень користувачів у служби оператора зв'язку, виражене у відсотках
12.	Частка користувачів, що виразили задоволеність якістю послуг зв'язку в цілому, %	Відношення числа користувачів, що виразили задоволеність якістю послуги зв'язки в цілому, до загальної кількості опитаних користувачів, виражене у відсотках
13.	Кваліфікація працівників служб оператора зв'язку, %	Відношення числа користувачів, що виразили задоволеність якістю роботи працівників служб операторів зв'язки в цілому, до загальної кількості опитаних користувачів, виражене у відсотках

КНД 45-067-97. Нормативи показників якості обслуговування викликів і якості встановлених телефонних з'єднань у телефонній мережі загального користування України.

КНД 45-056-97. Тимчасові нормативи показників якості телефонних з'єднань стаціонарних абонентів із телефонною мережею загального користування за допомогою радіо засобів.

СОУ 61-34620942-011:2012. Телекомунікаційні мережі передачі даних загального користування. Телекомунікаційні послуги. Основні показники якості. Методи випробування.

2.1.3. Пропускна здатність телекомунікаційних мереж

Пропускна здатність елементів мережі (напрямків або гілок зв'язку) може визначатися числом каналів у цих елементах чи максимально можливим навантаженням, яке може обслужити (пропустити) елемент

мережі. У цифрових первинних мережах теоретична [за формулою К. Шенона $C = \Delta F_{НК} \log_2 \left(1 + h^2\right)$] пропускна здатність дорівнює максимальної швидкості передачі в каналі або в тракті. Пропускна здатність (bandwidth) – це кількісна характеристика, що відображає можливості передачі даних у конкретному елементі мережі. **Фактична пропускна здатність мережі визначається комбінацією наступних факторів:**

– Властивості фізичних засобів підключення.
– Технології передачі й виявлення сигналів у мережі.

Однак з позиції користувача оцінка пропускної здатності числом каналів або максимальною швидкістю передачі інформації буде неточною, тому що не враховує вимог абонентів до якості обслуговування заявок. Тому для цих мереж реальна пропускна здатність може оцінюватися обсягом інформації, що передається від джерел інформації до споживачів при заданих ймовірносно-часових обмеженнях, обумовлених вимогами до якості обслуговування, її називають *продуктивністю (throughput)*.

Через безліч факторів продуктивність (throughput) звичайно не відповідає заявленій пропускній здатності (bandwidth) у реалізаціях на фізичному рівні. **На продуктивність впливає ряд факторів, у тому числі наступні:**

– Обсяг трафіка.
– Тип трафіка.
– Сумарна затримка, що залежить від кількості мережних пристроїв між джерелом і пунктом призначення.

Отже, продуктивність напрямку зв'язку Y_{ij} (p) дорівнює виконаному в цьому напрямку навантаженню Y_{ij} при виконанні вимог по якості обслуговування p :

$$Y_{ij} = Z_{ij} (1 - p_{ij}).$$

Продуктивність телекомунікаційної мережі оцінюється за результатами функціонування кожного напрямку зв'язку. Сумарна продуктивність усіх напрямків зв'язку визначає обсяг повідомлень чи навантаження в (Ерлангах), які пройшли через мережу від джерел до споживачів інформації, тобто продуктивність телекомунікаційної мережі в цілому.

Таким чином, можна сформулювати наступне визначення розглянутої характеристики: *продуктивністю телекомунікаційної мережі* називають сумарне навантаження, яке виконується в одиницю часу в усіх напрямках зв'язку, при забезпеченні заданих показників якості обслуговування.

Ілюстрація даного визначення представлена на рисунку 2.6.

Якщо в кожному напрямку зв'язку J_{ij}, де $i,j \in N$, значення виконаного навантаження дорівнює Y_{ij}, а показник якості обслуговування p_{ij}, то розподіл продуктивності $Y(P)$ мережі по напрямках зв'язку найбільше повно відображається наступною матрицею:

$$Y(P) = \begin{vmatrix} Y_{11}(p_{11}) & Y_{12}(p_{12}) & \dots & Y_{1j}(p_{1j}) & \dots & Y_{1N}(p_{1N}) \\ Y_{21}(p_{21}) & Y_{22}(p_{22}) & \dots & Y_{2j}(p_{2j}) & \dots & Y_{2N}(p_{1N}) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ Y_{i1}(p_{i1}) & Y_{i2}(p_{i2}) & \dots & Y_{ij}(p_{ij}) & \dots & Y_{iN}(p_{iN}) \\ \dots & \dots & \dots & \dots & \dots & \dots \\ Y_{N1}(p_{N1}) & Y_{N2}(p_{N2}) & \dots & Y_{Nj}(p_{Nj}) & \dots & Y_{NN}(p_{NN}) \end{vmatrix}.$$

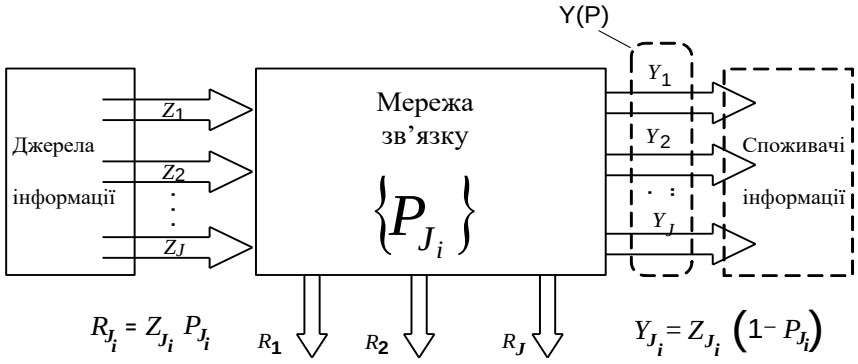


Рисунок 2.6 – Ілюстрація визначення продуктивності телекомунікаційної мережі

Чисельне значення продуктивності *Y(p)* мережі може бути отримане з виразу:

$$Y(P) = \sum_{i=1}^{N} \sum_{j=1}^{N} Y_{ij}(p_{ij}), \quad \forall\, i \neq j$$

де N – число комутаційних центрів у мережі.

Основними факторами, які визначають значення продуктивності кожного напрямку зв'язку і телекомунікаційної мережі в цілому, є значення пропускної здатності гілок, тип потоку заявок, алгоритм розподілу заявок у напрямках зв'язку і прийнята система обслуговування.

2.1.4. Живучість телекомунікаційних мереж

У процесі функціонування мереж зв'язку на них можуть виникати різні екстремальні ситуації, причинами яких є різнорідні зовнішні фактори, наприклад стихійні лиха (землетруси, повені, пожежі і т.п.), вплив агресивного зовнішнього середовища (супротивника, зброї масової поразки). У результаті цього можуть уражатися як окремі елементи, так і цілі ділянки цих мереж. Такі ситуації характеризуються різким зниженням пропускної здатності мереж зв'язку, а також їх структурно-топологічними змінами (аж до розриву зв'язаності), тобто порушенням зв'язку між визначеними пунктами мережі.

Дані про можливості мережі зв'язку по встановленню з'єднань і передачі (хоча б одиничних) повідомлень у зазначених ситуаціях дає

характеристика, яка дістала назву живучість мереж зв'язку. Таким чином, під живучістю мережі зв'язку розуміється її властивість забезпечувати встановлення з'єднань і передачу повідомлень між підключеними до неї джерелами і споживачами інформації при виході з ладу (в умовах зовнішнього впливу) її елементів або ділянок без нормування якості обслуговування. Живучість є однією з трьох властивостей ТКС (технічна надійність, живучість і перешкодостійкість), що визначають її стійке функціонування.

Фактори, які визначають живучість мереж зв'язку, можуть бути розділені на дві групи: з одного боку – впливом процесів і явищ, які викликають вихід з ладу елементів мережі зв'язку, а з іншого – організаційними заходами, які приймаються з метою виключення впливу таких процесів і явищ та властивостями мережі, які підвищують зв`язність структури мережі.

У першу групу факторів входять:

– агресивні прояви навколишнього середовища;

– шкідливий вплив об'єктів і штучних споруджень, розташованих поблизу елементів мережі зв'язку (вплив високих напруг і радіоперешкод, шкідливий вплив навколишнього середовища);

– вплив зброї супротивника;

– недостатня живучість елементів мережі зв'язку.

До другої групи факторів відносяться:

– раціональна побудова структури і топології мережі зв'язку;

– використання високонадійної і живучої апаратури зв'язку і засобів керування зв'язком;

– застосування спеціальних мір захисту елементів мережі зв'язку.

Виділяють два види живучості мережі зв'язку – структурну і функціональну. Перший вид визначає верхню (теоретично досяжну) границю живучості. Вважають, що мережа має *структурну живучість,* якщо можна вважати (з визначеною ймовірністю), що граф мережі, який описує її структуру, залишиться зв'язним після впливу на цю мережу визначених агресивних зовнішніх факторів, тобто якщо в зазначених умовах у кожному напрямку зв'язку зберігається (з визначеною ймовірністю) хоча б один шлях встановлення з'єднань, який забезпечує передачу повідомлень між кінцевими КЦ. Пошук шляху в розглянутому випадку здійснюється за структурою мережі. Цю задачу можна вважати тотожною відомій з теорії графів задачі пошуку шляхів на графі.

У реальній мережі зв'язку не кожний шлях, визначений за її графом, може бути використаний для передачі повідомлень. Це обумовлюється обмеженнями, які накладаються функціональними можливостями засобів зв'язку. Такими обмеженнями можуть бути використання неповнодоступних схем пошуку шляхів на комутаційних центрах (як кінцевих, так і транзитних), а також гранично припустиме число переприйомів, встановлене для даного типу систем передачі. Властивість мережі зв'язку забезпечувати встановлення з'єднань і передачу повідомлень у напрямках зв'язку при

ураженнях її елементів і ділянок у результаті зовнішніх впливів, з урахуванням функціональних можливостей засобів зв'язку на цих напрямках, називається *функціональною живучістю* даної мережі. Саме параметри функціональної живучості враховуються в першу чергу при оцінці можливостей мереж зв'язку.

За показник кількісної оцінки живучості окремих елементів мережі (комутаційних центрів, ліній зв'язку) приймається ймовірність їх виживання W, значення якої визначається експертно. За показник живучості напрямків зв'язку – ймовірність збереження зв'язаності в цих напрямках W_{ij}. Дані ймовірності W_{ij} визначаються шляхом використання основних законів теорії ймовірностей з урахуванням ймовірностей виживання кожного з елементів W, які входять до цього напрямку. Показником живучості мережі зв'язку буде сукупність показників живучості всіх напрямків зв'язку даної мережі, яка може бути представлена у вигляді матриці $|W|$ з елементами W_{ij}:

$$W = \begin{vmatrix} W_{11} & W_{12} & \dots & W_{1j} & \dots & W_{1N} \\ W_{21} & W_{22} & \dots & W_{2j} & \dots & W_{2N} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ W_{i1} & W_{i2} & \dots & W_{ij} & \dots & W_{iN} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ W_{N1} & W_{N2} & \dots & W_{Nj} & \dots & W_{NN} \end{vmatrix}.$$

Структурну живучість мережі позначають як $W(G)$, а функціональну живучість – $W(F)$.

Живучість W_{ij}^{μ} будь-якого шляху встановлення з'єднання, який складається з сукупності послідовно включених елементів (комутаційних центрів, гілок), визначається добутком:

$$W_{ij}^{\mu} = \prod_{n=1}^{N} W_n \prod_{m=1}^{M} W_m , \qquad (1)$$

де N – число КЦ у шляху μ;
W_n – ймовірність виживання n –го КЦ у заданих умовах;
M – число гілок у шляху μ;
W_m – ймовірність виживання m –тої гілки в заданих умовах.

При наявності в напрямку зв'язку декількох незалежних шляхів передачі інформації його живучість зберігається, якщо при поразці елементів (чи ділянок) зберігається працездатним хоча б один з цих шляхів:

$$W_{НЗ} = 1 - \prod_{\mu=1}^{\chi} \left(1 - W_{ij}^{\mu}\right), \qquad (2)$$

де χ – число незалежних шляхів у напрямку зв'язку.

Наведені формули розрахунку структурної живучості відносяться до методу точного визначення значення живучості, який отримав назву *метод повного перебору*. Проте сучасні мережні протоколи мають можливість застосування залежних шляхів. Тому необхідно враховувати їх потенційні можливості по використанню ресурсів мережі. В цьому випадку процес розрахунку стає більш трудомісткою операцією, яка не може бути реалізована навіть за допомогою сучасних обчислювальних засобів. Тому існують як методи точного розрахунку живучості (ймовірності зв'язності) напрямів передачі із залежними шляхами, так і наближені методи оцінки.

2.1.5. Надійність функціонування телекомунікаційних мереж

Характеристика, що визначає можливість абонентів обмінюватися інформацією у мережах зв'язку в умовах виникнення технічних відмовлень і експлуатаційних помилок на її елементах без помітного погіршення ймовірносно-часових показників обслуговування заявок, одержала назву надійності функціонування цих мереж. У зв'язку з цим під ***надійністю функціонування*** телекомунікаційної мережі розуміється її властивість забезпечувати встановлення з'єднань і передачу повідомлень у реальних умовах експлуатації при збереженні заданих значень показників якості обслуговування, встановленого для кожного напрямку зв'язку.

У загальному випадку надійність функціонування мережі зв'язку визначається надійністю її елементів, структурою і топологією мережі, а також станом навколишнього середовища. У зв'язку з тим, що функціонально мережа зв'язку розбивається на напрямки зв'язку, кожному з яких може бути властива (задана) своя якість обслуговування заявок, що надходять до нього, надійність функціонування оцінюється окремо для кожного з цих напрямків. Сукупність показників надійності функціонування всіх напрямків зв'язку, характеризує надійність функціонування розглянутої мережі в цілому. Формально незалежна оцінка надійності функціонування різних напрямків зв'язку не означає їх функціональну незалежність. Це обумовлюється тим, що ті самі елементи мережі зв'язку входять у різні напрямки зв'язку.

Як показник надійності функціонування телекомунікаційної мережі і її основних елементів (напрямків зв'язку і гілок, що входять у ці напрямки) приймається ймовірність P*(t)* безвідмовного обслуговування заявок, що надходять у мережу. Для елемента мережі зв'язку, ймовірність безвідмовного обслуговування може бути визначена як:

$$P_{n,m}(t) = R_{n,m}(1 - p_{n,m}),$$

де $R_{n,m}$ – ймовірність безвідмовної роботи елемента;
$p_{n,m}$ – втрати заявок на даному елементі.

Ймовірність безвідмовної роботи R, що входить у цій вираз і визначає технічний стан утворюючих, наприклад, гілку засобів зв'язку. Величина R може бути визначена таким чином:

$$R = k_г\, e^{-t/T},$$

де – коефіцієнт готовності гілки виконувати належну їй задачу;
t – час виконання цієї задачі;
T – середній час роботи засобів гілки до технічного відмовлення (середній час напрацювання на відмовлення).

Значення параметрів $k_г$ і T, як правило, визначаються технічним нормуванням використовуваних засобів зв'язку. Параметр t у більшості випадків обумовлюється організаційними міркуваннями. Параметр $k_г$ може бути також вирахуваний, виходячи з даних про можливість відновлення працездатності (заміни) обладнання:

$$\mathrm{k_г} = \frac{\mathrm{T}}{\mathrm{T}+\mathrm{T_в}},$$

де $\mathrm{T_в}$ – час на відновлення працездатності (заміну) обладнання.

У випадку необхідності розрахунку надійності шляху передачі інформації або напрямку зв'язку в цілому цілком можливо використання формул виведених для живучості (1) та (2), в яких у якості показників елементів будуть використані показники надійності $\mathrm{P}_{n,m}(t)$.

2.2. Постановка та методи рішення задач розрахунку основних параметрів ТКМ

2.2.1. Постановка задач розрахунку параметрів ТКМ

Задача розрахунку параметрів пропускної здатності ТКМ

При дослідженнях телекомунікаційних мереж за параметрами пропускної здатності можуть вирішуватися дві задачі: пряма і зворотна.

Пряма задача передбачає визначення якості обслуговування P_{HC} і виконаного навантаження Y_{HC} у напрямках зв'язку. Формулюється задача в такий спосіб: оцінити відповідність реальної (очікуваної) продуктивності її нормованому значенню для кожного напрямку зв'язку (інформаційного напрямку).

Для рішення прямої задачі, як правило, використовуються наступні вихідні дані:

1. Структура мережі, задана матрицею зв'язаності $A = \{a_{ij}\}$ або графом $G\,(N, M)$.

2. Величина навантаження $Z_{HC} = \{Z_{ij}\}$, що надходить у кожен напрямок зв'язку для обслуговування в ГНН.

3. Канальна ємність гілок мережі $V = \{v_{ij}\}$.

4. Алгоритм вибору шляхів встановлення з'єднань у напрямках зв'язку.

Вирішується вона в два етапи.

Перший етап. Визначають якість обслуговування заявок у кожному напрямку зв'язку (або інформаційному напрямку):

$$P_{HC} = F\,(Z,\ V).$$

Тобто якість обслуговування визначається через втрати в напрямках зв'язку.

За отриманим значенням P_{HC} у кожному напрямку зв'язку здійснюється оцінка відповідності реальної (очікуваної) якості обслуговування заявок її нормованому значенню. Якщо вимоги по якості обслуговування виконуються, то переходять до другого етапу.

Другий етап. Визначають величину виконаного навантаження в кожному напрямку зв'язку:

$$Y_H = Z_H\,(1\text{-}P_{HC}).$$

А як випливає з визначення, це і є пропускна здатність.

Зворотна задача формулюється в таким чином: визначити необхідне число каналів у гілках телекомунікаційної мережі (необхідний ресурс мережі), що забезпечить задані (нормовані) значення продуктивності її напрямків зв'язку (інформаційних напрямків):

$$V = \Psi\,(Z_H,\ P_{HC}) \rightarrow Y_H(P_{HC}) = \Phi\,(V,\ Z_H).$$

Вихідними даними для рішення цієї задачі, як правило, є:

1. Структура мережі, задана матрицею зв'язаності $A = \{a_{ij}\}$ або графом $G(N, M)$.

2. Величина навантаження $Z_{HC} = \{Z_{ij}\}$, що надходить у кожен напрямок зв'язку для обслуговування в ЧНН.

3. Максимально припустимі ймовірності втрат у напрямках зв'язку, що задані матрицею $P_{HC} = \{P_{ij}\}$.

4. Алгоритм вибору шляхів установлення з'єднань у напрямках зв'язку.

Задача розрахунку надійності функціонування ТКМ

Під надійністю $W_{ij}(t)$ функціонування розуміється властивість телекомунікаційної мережі забезпечити встановлення з'єднань і передачу повідомлень у реальних умовах експлуатації при збереженні значень показників якості обслуговування, встановлених для кожного напрямку зв'язку.

На практиці, як правило, вирішується тільки пряма задача, а саме задача аналізу надійності функціонування телекомунікаційної мережі. Як і

задача оцінки продуктивності, задача оцінки надійності функціонування телекомунікаційної мережі задається й оцінюється по напрямках зв'язку.

Формулюється задача в таким чином – розрахувати надійності функціонування напрямків зв'язку телекомунікаційної мережі і порівняти з заданою (нормованою) величиною.

Вихідними даними для розрахунку надійності функціонування телекомунікаційної мережі можуть бути:

t – безперервний час виконання завдання;

T_m – середній час безвідмовної роботи гілки (засобу зв'язку);

$T_{тв}$ – середній час відновлення ушкодженої гілки (засобу зв'язку);

$k_{гт}$ – коефіцієнт готовності гілки (засобу зв'язку);

R_m – ймовірність безвідмовної роботи гілки (засобу зв'язку).

Задача розрахунку живучості ТКМ

Під живучістю $W(G)$ телекомунікаційної мережі розуміється властивість забезпечувати встановлення з'єднань і передачу повідомлень у всіх напрямках зв'язку при виході з ладу елементів або дільниць мережі в умовах агресивних зовнішніх впливів, хоча б і з погіршенням якості обслуговування.

Показником живучості телекомунікаційної мережі є ймовірність збереження хоча б одного шляху встановлення з'єднання, що забезпечує передачу повідомлень у кожному напрямку зв'язку.

Живучість телекомунікаційної мережі, яка враховує тільки ймовірність зв'язаності її структури, одержала назву структурної живучості.

У реальній мережі не кожен шлях, що є у структурі телекомунікаційної мережі, може бути використаний для передачі повідомлень. Це обумовлюється обмеженнями, що накладаються функціональними можливостями використовуваних засобів зв'язку. У зв'язку з цим живучість, яка враховує можливості структури мережі та обмеження, що накладаються функціональними можливостями використовуваних засобів зв'язку, має назву функціональна живучість телекомунікаційної мережі.

При розгляді питань живучості вирішується пряма задача – аналізу живучості телекомунікаційної мережі.

Як і задача оцінки надійності, живучість задається й оцінюється по напрямках зв'язку.

Постановка задачі формулюється в таким чином – розрахувати живучість напрямків зв'язку і порівняти з заданими (нормованими) значеннями.

Розрахунок може вестися як для структурної, так і для функціональної живучості. На практиці, як правило, визначається функціональна живучість.

Вихідними даними для розрахунку є значення живучості елементів телекомунікаційної мережі.

2.2.2. Методи розрахунку параметрів ТКМ

Розрахунок продуктивності некомутованої телекомунікаційній мережі

Розрахунок продуктивності розглянемо на прикладі простої три вузлової мережі, структура і топологія якої має вигляд, представлений на рисунку 2.7.

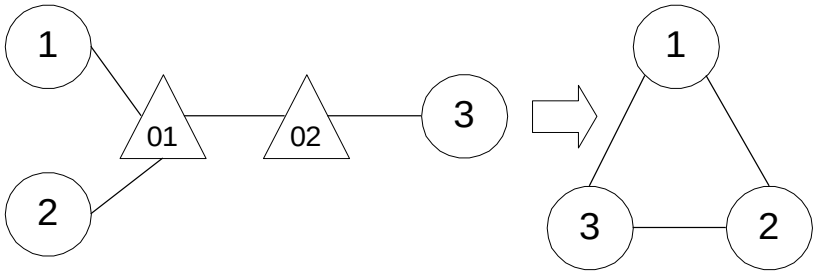


Рисунок 2.7 – Структура та топологія три вузлової мережі

Початкові дані для розрахунку:

1. Структура і топологія мережі, описується графом, представленим на рисунку 2.7.

2. Величина навантаження, що поступає в кожен напрям зв'язку, має такі значення $\{Z_{ij}\}$:

$$Z_{12}=0,7\text{Ерл};\ Z_{13}=3,1\text{Ерл};\ Z_{23}=0,9\text{Ерл}.$$

3. Вимоги до якості обслуговування в кожному напрямі зв'язку, описуються наступними значеннями $\{P_{ij}\}$:

$$P_{12} = 5‰;\ P_{13} = 10‰;\ P_{23} = 10‰.$$

Основні умови, обмеження і допущення:

1. Телекомунікаційна мережа з явними втратами.

2. Потоки заявок, що поступають на обслуговування в кожен напрям зв'язку, є простими.

3. Час встановлення з'єднання з'єднань в напрямах зв'язку рівний нулю.

Необхідно визначити необхідну канальну ємкість $V = \{V_{ij}\}$ гілок на структурі і топології мережі, що забезпечують виконання вимог по пропускній спроможності.

Рішення:

1. За допомогою відповідних таблиць визначаємо необхідне число каналів на структурі телекомунікаційної мережі, що забезпечують виконання вимог по пропускній спроможності $\{V_m\}$:

$$V_{12} = 4;\ V_{13} = 8;\ V_{23} = 5.$$

2. Розраховуємо необхідне число каналів на топології телекомунікаційної мережі:

$$V_{1\text{-}01} = 8 + 4 = 12;\ V_{2\text{-}01} = 4 + 5 = 9;$$
$$V_{01\text{-}02} = 8 + 5 = 13;\ V_{02\text{-}3}=8+5=13.$$

Розрахунок закінчений.

Порядок розрахунку продуктивності комутованої телекомунікаційної мережі. Пряме завдання

Постановка завдання

Пряме завдання передбачає визначення виконаного ТКМ навантаження Y і якості обслуговування q для кожного напряму зв'язку і порівняння набутих значень із заданими нормами.

Це завдання аналізу. Вона вирішується для ТКМ що вже знаходиться в експлуатації або після закінчення проектування мережі з метою перевірки виконання вимог, що пред'являються до їх функціонування.

Початковими даними для вирішення завдання є:

1. Структура мережі, задана матрицею зв'язності $A=\{a_{ij}\}$ або графом G(N,M).
2. Величина навантаження $Z = \{Z_{ij}\}$, зв'язку, що поступає в кожен напрям, для обслуговування в ЧНН.
3. Канальна ємкість гілок мережі $V = \{v_{ij}\}$.
4. Алгоритм вибору шляхів встановлення з'єднань в напрямах зв'язку.

В результаті рішення завдання повинні бути визначені:

1. Якість обслуговування заявок q в кожному напрямі зв'язку: $q = 1 – p$.
2. Пропускна спроможність кожного напряму зв'язку $Y_{ij}(p)= Z_{ij} (1 – p_{ij})$.

В процесі рішення використовується ряд допущень:

1. Потік викликів, що поступають на обслуговування в кожен напрям зв'язку, є простим.
2. Система знаходиться в стані статистичної рівноваги.
3. Система приймається з втратами.
4. Втрати, що виникають в КЦ із-за зайнятості обслуговуючих приладів і блокування в комутаційному полі, малі в порівнянні з втратами із-за зайнятості каналів в гілках мережі і не враховуються.
5. Вірогідність зайнятості каналів всіх гілок мережі взаємно незалежні.
6. Час встановлення з'єднання рівний нулю.

Основні етапи розрахунку продуктивності комутованої телекомунікаційної мережі

Рішення цієї задачі припускає виконання ряду етапів, кожен з яких є окремою самостійною підзадачею. Це:

1. Визначення сукупності шляхів передачі інформації в напрямах зв'язку.

2. Розподіл навантаження по шляхах першого вибору і визначення орієнтовних значень якості обслуговування на гілках мережі.

3. Корекція значень вірогідності втрат і навантаження на гілках мережі.

4. Визначення якості обслуговування і виконаного навантаження в напрямах зв'язку і порівняння із заданими вимогами.

Етап 1. Визначення сукупності шляхів передачі інформації в напрямках зв'язку

З метою збільшення живучості, надійності і якості обслуговування в ТКМ у кожному напрямку зв'язку передбачається кілька шляхів передачі інформації. Визначення цієї сукупності шляхів передачі інформації здійснюється за структурою мережі зв'язку. Для зменшення розмірності задачі доцільно структуру мережі, яка описується графом $G(N, M)$, розбити на два підграфи: $G^T(N^T, M^T)$ і $G^O(N^O, M^O)$. При цьому повинно виконуватися умова:

$$G(N, M) = G^T(N^T, M^T) \not| G^O(N^O, M^O).$$

До графа $G^T(N^T, M^T)$ відносять частину мережі, що складається з транзитних комутаційних центрів і з'єднуючих їх гілок. Усі КЦ $\in G^T(N^T, M^T)$ мають не менш двох інцидентних гілок.

До графу $G^O(N^O, M^O)$ відносять сукупність кінцевих КЦ з інцидентними їм гілками. Усі КЦ $\in G^O(N^O, M^O)$ мають, як правило, одну інцидентну гілку.

Сукупність шляхів передачі інформації визначається відносно КЦ $\in G^T(N^T, M^T)$, тому що тільки ця частина мережі забезпечує кілька шляхів передачі інформації в напрямках зв'язку.

Шляхи можуть бути незалежними і залежними. Використання залежних шляхів передачі інформації вимагає вживання спеціальних заходів боротьби з виникненням "петель", що веде до збільшення службового навантаження на мережу зв'язку й ускладненню керуючих пристроїв КЦ. Передача інформації з незалежних шляхів вільна від цього недоліку. Крім того, використання більш двох обхідних шляхів не приводить до істотного ефекту. Тому якщо структура мережі зв'язку, яка описується графом $G^T(N^T, M^T)$, дозволяє організувати 2 і більш незалежних шляхів встановлення з'єднання, то використання залежних шляхів у ряді випадків недоцільно.

Задача визначення сукупності незалежних шляхів встановлення з'єднань у напрямках зв'язку може вирішуватися різними шляхами:

1. Візуально, на підставі структури мережі;

2. За допомогою аналітичних методів, наприклад, по модифікованій матриці зв'язаності методом послідовного зведення її в ступінь.

Визначена одним з перерахованих способів сукупність незалежних шляхів представляється у вигляді матриці маршрутів $||M||$:

$$M=||\mu^{\nu}_{ij}||,$$

де: μ^{ν}_{ij} – склад гілок, що входять у шлях встановлення з'єднання;
ν – номер шляху встановлення з'єднання.

Етап 2. Розподіл навантаження по шляхах першого вибору і визначення орієнтованих значень якості обслуговування на гілках мережі

Вихідними даними для рішення цієї задачі є матриця маршрутів, визначена на першому етапі розв'язання задачі й алгоритм вибору шляхів передачі інформації в кожному напрямку зв'язку.

Спрощений алгоритм рішення задачі наступний:

1. Вибирається будь-який напрямок зв'язку J_{ij} наприклад, що має мінімальний номер.

2. По алгоритму вибору шляхів передачі інформації в напрямках зв'язку (вихідні дані) визначаються гілки шляху першого вибору.

3. Визначається навантаження Z_{ij}, що надходить на обслуговування в даний напрямок зв'язку, і її значення приписується всім гілкам шляху першого вибору.

4. Вибирається наступний напрямок зв'язку і виконуються операції відповідно до п. 1...3 доти, поки не буде розподілене навантаження в усіх напрямках зв'язку.

5. Визначається сумарне значення z_{mij} навантаження, яке обслуговується кожною гілкою, шляхом підсумовування приписаних їм значень навантаження, що надходять із усіх напрямків зв'язку. Отриманий результат записується у відповідну матрицю $Z_m = \{z_{mij}\}$.

Відповідно до рекомендацій іноді при розрахунках продуктивності ТКМ доцільно оперувати не математичним чеканням z_m навантаження, а його розрахунковим z_{mp} значенням, яке визначається таким чином:

$$Z_{mp} = Z_m + \eta\sqrt{Z_m},$$

де η = 0,6742 – коефіцієнт, що враховує коливання середнього значення навантаження.

Отримані результати записуються у відповідну матрицю $Z_{mp} = \{z_{mpij}\}$.

6. За розрахованим значенням z_{mij} або z_{mpij} та заданою кількістю каналів у кожній гілці мережі зв'язку визначаються ймовірності втрат на цих гілках по відомих залежностях:

$$p_{mij} = f(V_{mij}, z_{mij}).$$

Отримані значення записуються в матрицю $P_m = \{p_{mij}\}$ втрат на гілках мережі.

Етап 3. Корекція значень ймовірності втрат і навантаження на гілках мережі

Отримані на попередньому етапі значення величини навантаження і ймовірності втрат на гілках мережі є орієнтованими, тому що вони розраховані без обліку навантаження, що надходить на обслуговування в шляхи других і наступних виборів. Тому необхідно зробити корекцію значень навантаження і ймовірності втрат на гілках мережі з урахуванням цього фактору.

Вихідними даними для рішень цієї задачі є матриці маршрутів (перший етап), втрат (другий етап) і алгоритм вибору шляхів передачі інформації в напрямках зв'язку. **Корекція розподілу навантаження по гілках мережі, здійснюється таким чином:**

1. З усієї сукупності напрямків вибирається яке-небудь з них, наприклад, з найбільшим заданим навантаженням.

2. Для обраного напрямку зв'язку відшукується шлях першого вибору.

3. Першій гілці цього шляху приписується значення навантаження Z_{ij}, що дорівнює навантаженню, даного напрямку; другій гілці - *значення* $Zij\ (l - p_{m1})$, *де* p_{m1} - ймовірність втрат, визначена для першої гілки шляху; третій гілці - *значення* $Z_{ij}\ (l - p_{m1})\ (1 - p_{m2})$, *де* p_{m2} - ймовірність втрат, визначена для другої гілки шляху, і т.д.

4. Для того ж напрямку зв'язку обирається шлях другого вибору, у першу гілку якого надходить наступне навантаження:

$$Z_{ij} \cdot [1 - \prod_{l=1}^{k} (1 - p_{ml})],$$

де p_{ml} – втрати на гілках шляху першого вибору.

Другій і наступній гілкам шляху другого вибору приписуються значення навантажень так само, як для гілок шляху першого вибору. У таким же чином здійснюються операції з гілками шляхів наступних виборів.

5. У послідовності, викладеної для першого напрямку зв'язку, здійснюється розподіл навантаження для всіх інших напрямків зв'язку.

6. Значення навантаження від кожного напрямку зв'язку, приписані гілкам, складаються по кожній гілці. Отриманий результат записується у відповідну матрицю $Z_m = \{z_{mij}\}$.

Сумарне значення навантаження по всіх гілках мережі зв'язку являє собою функціонуюче навантаження.

За розрахованим значенням z_{mij}, (а при необхідності по z_{mpij}) і заданою кількістю каналів у кожній гілці мережі зв'язку визначаються ймовірності втрат на цих гілках:

$$p_{mij} = f(V_{mij}, z_{mij})$$

Отримані значення записуються в матрицю $P_m = \{p_{mij}\}$ втрат на гілках мережі.

Для одержання остаточних результатів із заданою точністю на даному етапі виконується ітераційна процедура повторення розрахунків. Практично число ітерацій у більшості випадків не перевищує двох трьох.

Етап 4. Визначення якості обслуговування і виконаного навантаження в напрямках зв'язку і порівняння з заданими вимогами

Рішення цієї задачі передбачає виконання наступних операцій:

1. Для кожного напрямку зв'язку складається розрахунковий паралельно-послідовний граф шляхів встановлення з'єднань. Його ребрам приписуються відповідні значення ймовірностей втрат p_{mij} на гілках.

2. За отриманими графами, для кожного напрямку зв'язку J_{ij}, складається розрахунковий вираз. Якщо в напрямку зв'язку мається тільки один шлях встановлення з'єднання із к гілок, ймовірність втрат P_{ij} у ньому дорівнює:

$$P_{ij} = 1 - \prod_{n=1}^{k} (1 - p_{m_n}).$$

Якщо в напрямку зв'язку мається χ незалежних шляхів установлення з'єднання, то ймовірність втрат у ньому дорівнює:

$$P_{ij} = \prod_{l=1}^{\chi} \left[1 - \prod_{n=1}^{k} (1 - p_{m_{nl}}) \right].$$

3. Розраховуються значення P_{ij} для кожного J_{ij} напрямку зв'язку і записуються в матрицю $P = \{P_{ij}\}$.

4. За відомим значенням навантаження Z_{ij}, *що* надходить на обслуговування в кожний напрямок зв'язку J_{ij}, і значенню показника якості обслуговування в ньому P_{ij} визначається величина продуктивності:

$$Y_{ij}(p) = Z_{ij}\,(1\text{-}P_{ij})$$

Розраховані значення записуються в матрицю продуктивності напрямків зв'язку розглянутої мережі:

$$Y(p) = \{Y_{ij}(p)\}$$

5.Отримані результати порівнюються з заданими вимогами.

Порядок розрахунку канальної ємності гілок телекомунікаційної мережі, що комутується. Зворотна задача оцінки пропускної здатності

Постановка задачі і формулювання вихідних даних.

При проектуванні телекомунікаційної мережі широко застосовується рішення зворотної задачі оцінки пропускної здатності, а саме – визначення потужності V_{mij} гілок за заданим значенням якості обслуговування в напрямках зв'язку. **Вихідними даними при рішенні цієї задачі є:**

1. Структура мережі, задана матрицею зв'язаності $A= \{a_{ij}\}$ або графом $G(N,M)$.

2. Величина навантаження $Z = \{Z_{ij}\}$, *що* надходить у кожний напрямок зв'язку для обслуговування в ГНН.

3. Максимально припустимі ймовірності втрат у напрямках зв'язку, що задані матрицею $P = \{P_{ij}\}$.

4. Алгоритм вибору шляхів встановлення з'єднань у напрямках зв'язку.

Визначити:

1. Необхідну канальну ємність $V = \{V_{ij}\}$ гілок мережі, що забезпечує задану пропускну здатність телекомунікаційної мережі.

У процесі рішення використовується ряд допущень:

1. Потік викликів, що надходять на обслуговування в кожний напрямок зв'язку, є найпростішим.

2. Система знаходиться в стані статистичної рівноваги.

3. Система приймається з явними втратами.

4. Втрати, що виникають у КЦ внаслідок зайнятості обслуговуючих приладів і блокування у комутаційному полі, малі в порівнянні з втратами внаслідок зайнятості каналів у гілках мережі і не враховуються.

5. Ймовірність зайнятості каналів усіх гілок мережі взаємно незалежні.

6. Час установлення з'єднання дорівнює нулю.

Етапи розрахунку канальної ємності гілок ТКМ, що комутується

Рішення даної задачі являє собою виконання ряду етапів, кожний з яких передбачає розгляд окремої самостійної підзадачі:

1. Визначення сукупності шляхів передачі інформації в напрямках зв'язку.

2. Нормування значень якості обслуговування на гілках мережі.

3. Розподіл навантаження по гілках, що складає шляхи перших і наступних виборів.

4. Визначення числа каналів у гілках мережі і при необхідності їх типізація.

5. Корекція значень ймовірності втрат на гілках мережі.

6. Перевірочний розрахунок значень ймовірностей втрат і виконаного навантаження в напрямках зв'язку.

Розглянемо основний зміст перерахованих вище етапів.

Етап 1. Визначення сукупності шляхів передачі інформації в напрямках зв'язку

З метою збільшення живучості, надійності і якості обслуговування в ТКМ у кожному напрямку зв'язку передбачається кілька шляхів передачі інформації. Визначення цієї сукупності шляхів передачі інформації здійснюється за структурою мережі зв'язку. Для зменшення розмірності задачі доцільно структуру мережі, яка описується графом *G(N, M),* розбити на два підграфи: $G^T(N^T, M^T)$ *і* $G^O(N^O, M^O)$. При цьому повинно виконуватися умова:

$$G(N, M) = G^T(N^T, M^T) \not| G^O(N^O, M^O).$$

До графа $G^T(N^T, M^T)$ відносять частину мережі, що складається з транзитних комутаційних центрів і з'єднуючих їх гілок. Усі КЦ $\in G^T(N^T, M^T)$ мають не менш двох інцидентних гілок.

До графу $G^O(N^O, M^O)$ відносять сукупність кінцевих КЦ з інцидентними їм гілками. Усі КЦ $\in G^O(N^O, M^O)$ мають, як правило, одну інцидентну гілку.

Сукупність шляхів передачі інформації визначається відносно КЦ $\in G^T(N^T, M^T)$, тому що тільки ця частина мережі забезпечує кілька шляхів передачі інформації в напрямках зв'язку.

Шляхи можуть бути незалежними і залежними. Використання залежних шляхів передачі інформації вимагає вживання спеціальних заходів боротьби з виникненням "петель", що веде до збільшення службового навантаження на мережу зв'язку й ускладненню керуючих пристроїв КЦ. Передача інформації з незалежних шляхів вільна від цього недоліку. Крім того, використання більш двох обхідних шляхів не приводить до істотного ефекту. Тому якщо структура мережі зв'язку, яка описується графом $G^T(N^T, M^T)$, дозволяє організувати 2 і більш незалежних шляхів встановлення з'єднання, то використання залежних шляхів у ряді випадків недоцільно.

Задача визначення сукупності незалежних шляхів встановлення з'єднань у напрямках зв'язку може вирішуватися різними шляхами:

1. Візуально, на підставі структури мережі;

2. За допомогою аналітичних методів, наприклад, по модифікованій матриці зв'язаності методом послідовного зведення її в ступінь.

Визначена одним з перерахованих способів сукупність незалежних шляхів представляється у вигляді матриці маршрутів $||M||$:

$$M=||\mu^{\nu}_{ij}||,$$

де: μ^{ν}_{ij} – склад гілок, що входять у шлях встановлення з'єднання;
ν – номер шляху встановлення з'єднання.

Етап 2. Нормування значень якості обслуговування на гілках мережі

Мережа, що комутується, характеризується тим, що ймовірність втрат на будь-якій гілці, у загальному випадку, залежить від ймовірності втрат на всіх інших гілках. Цю залежність ймовірностей втрат на гілках мережі зв'язку з урахуванням визначеної сукупності незалежних шляхів у напрямках зв'язку (матриця ||M||) можна представити у вигляді системи нерівностей:

$$\begin{cases} P_{ij} \geq \prod\limits_{i=1}^{\nu}\left[1-\prod\limits_{j=1}^{n_\nu}\left(1-p_{ij}\right)\right], \\ P_{kl1} \geq \prod\limits_{k=1}^{\nu}\left[1-\prod\limits_{l=1}^{n_\nu}\left(1-p_{kl}\right)\right], \\ \text{..... ....}, \\ P_{mt} \geq \prod\limits_{m=1}^{\nu}\left[1-\prod\limits_{t=1}^{n_\nu}\left(1-p_{mt}\right)\right]. \end{cases} \qquad (3)$$

де ν - число незалежних шляхів у напрямку зв'язку;
n_ν – число гілок у ν-му шляху встановлення з'єднання;
p_{ij}, p_{kl}, ..., p_{mt} – припустимі ймовірності втрат на гілках;
P_{ij}, P_{kl}, ..., P_{mt} – припустимі величини втрат у відповідних напрямках зв'язку.

Число нерівностей системи визначається числом інформаційних напрямків у мережі.

Шуканими є ймовірності p_{ij}, p_{kl}, ..., p_{mt} – втрат на гілках; Рішення системи нерівностей (3) у прямій постановці є досить складною і трудомісткою задачею.

На практиці звичайно використовується наступний порядок її рішення:

1. Вибирають нерівність, що відповідає напрямкові зв'язку з найбільш жорсткими вимогами до якості обслуговування на гілках телекомунікаційної мережі (як правило, це напрямок зв'язку, що має мінімальне число обхідних шляхів, найкоротший шлях у якому має максимальну довжину, а вимоги до якості обслуговування найбільш високі):

$$P_{ij} \leq \prod_{i=1}^{\nu}\left[1-\prod_{j=1}^{n_\nu}\left(1-p_{mij}\right)\right] \qquad (4)$$

2. Переходять від нерівності до рівності, тобто:

$$P_{ij} = \prod_{i=1}^{\nu}\left[1-\prod_{j=1}^{n_\nu}\left(1-p_{mij}\right)\right] \qquad (5)$$

3. Припускають рівність втрат на всіх гілках за умови виконання вимог до якості обслуговування в напрямку зв'язку. У цьому випадку рівняння (5) може бути перетворене в рівняння (6):

$$P_{ij} = \left[1 - \left(1 - p_{cp1}\right)^{m_\nu}\right] \tag{6}$$

Це рівняння з одним невідомим і може бути вирішено, наприклад, методом підстановки.

4. Усім гілкам m_{ij} напрямку зв'язку J_{ij} привласнюється значення ймовірності втрат p_{cp1}, отримане в результаті рішення рівняння (6).

5. Із системи (3) вибирається наступна нерівність, що відповідає вимогам пункту 1 на даному етапі обчислень і має невідомі значення p_{mij}.

Розраховані на попередніх етапах ймовірності втрат на гілках входять у наступні рівняння зі своїми значеннями, а невідомі прирівнюються між собою.

6. Аналогічним образом вирішують друге і наступне рівняння доти, поки всім гілкам мережі не будуть привласнені розраховані для них значення ймовірностей утрат. Якщо одержують кілька значень ймовірностей втрат для однієї гілки, то їй привласнюється найменше з них. Результати розрахунку зводяться в матрицю $\{p_{mij}\}$.

Після визначення ймовірності p_{mij} втрат на всіх гілках m_{ij} ТКМ здійснюється перевірка відповідності якості обслуговування у всіх напрямках зв'язку пропонованим вимогам. З цією метою визначається Δ_{ij} різниця між нормованими і дійсними значеннями ймовірностей втрат у всіх напрямках зв'язку:

$$\Delta_{ij} = \left\{P_{ij} - \prod_{i=1}^{\nu}\left[1 - \prod_{j=1}^{m_\nu}\left(1 - p_{ij}\right)\right]\right\} \tag{7}$$

Дані величини повинні бути $\Delta_{ij} \geq 0$. Якщо в якому-небудь напрямку зв'язку $\Delta_{ij} < 0$, то значить у процесі рішення були порушені умови п.1 і необхідно повторно повернутися до рішення системи нерівностей (3). А це може привести до значного збільшення часу рішення задачі.

Виникнення помилок позв'язане з тим, що нерідко важко однозначно визначити напрямок зв'язку, що має найбільш жорсткі вимоги до якості обслуговування.

Усунути невизначеність можна використанням наступного алгоритму:

1. Визначається сукупність шляхів передачі інформації у всіх напрямках зв'язку.

2. Записується рівняння втрат і визначається усереднений показник якості обслуговування p_{cp} на гілках (за умови рівності втрат) для кожного напрямку.

3. Здійснюється ранжирування напрямків зв'язку по показнику p_{cp} (від $\min\ p_{cp}$ до $\max\ p_{cp}$).

Найбільш жорсткі вимоги до якості обслуговування на гілках мережі в тих напрямках зв'язку, у яких значення p_{cp} мінімальне на даному етапі розрахунків. Починаючи з цього напрямку зв'язку і необхідно здійснювати обчислювальні операції..

Етап 3. Розподіл навантаження по гілках, що складають шляхи першого і наступних виборів

Вихідними даними для рішення цієї задачі є матриці маршрутів $\{\mu^{v}_{ij}\}$ (перший етап) і втрат *{p_{mij}}* (другий етап) відповідно. Алгоритм вибору шляхів у напрямках зв'язку однозначно визначає порядок їх заняття. **Розподіл навантаження по гілках мережі, здійснюється таким чином:**

1. З усієї сукупності напрямків зв'язку вибирається яке-небудь з них, наприклад, з найбільшим заданим навантаженням, що надходить.

2. Для обраного напрямку зв'язку відшукується шлях першого вибору.

3. Першій гілці цього шляху приписується значення навантаження Z_{ij}, що дорівнює навантаженню, даного напрямку; другій гілці - *значення Zij (l - p_{m1}), де p_{m1}* - ймовірність втрат, визначена для першої гілки шляху; третій гілці - *значення Z_{ij} (l - p_{m1}) (1 - p_{m2}), де p_{m2}* - ймовірність втрат, визначена для другої гілки шляху, і т.д.

4. Для того ж напрямку зв'язку обирається шлях другого вибору, у першу гілку якого надходить наступне навантаження:

$$Z_{ij} \cdot [1 - \prod_{l=1}^{k} (1 - p_{ml})],$$

де p_{ml} – втрати на гілках шляху першого вибору.

Другій і наступній гілкам шляху другого вибору приписуються значення навантажень так само, як для гілок шляху першого вибору. У таким же чином здійснюються операції з гілками шляхів наступних виборів.

5. У послідовності, викладеної для першого напрямку зв'язку, здійснюється розподіл навантаження для всіх інших напрямків зв'язку.

6. Значення навантаження від кожного напрямку зв'язку, приписані гілкам, складаються по кожній гілці. Отриманий результат записується у відповідну матрицю $Z_m = \{z_{mij}\}$.

Сумарне значення навантаження по всіх гілках мережі зв'язку являє собою функціонуюче навантаження.

Етап 4. Визначення числа каналів у гілках мережі

Розраховані на попередніх етапах значення величини навантаження і ймовірностей втрат на гілках є вихідними даними для розрахунку числа

каналів. При цьому відповідно до рекомендацій іноді при розрахунках продуктивності ТКМ доцільно оперувати не математичним чеканням z_m навантаження, а його розрахунковим z_{mp} значенням, яке визначається таким чином:

$$Z_{mp} = Z_m + \eta\sqrt{Z_m},$$

де η = 0,6742 - коефіцієнт, що враховує коливання середнього значення навантаження.

Отримані результати записуються у відповідну матрицю $Z_{mp} = \{z_{mpij}\}$.

Відповідно до прийнятого допущення про те, що потоки заявок, що надходять на обслуговування, найпростіші, число каналів v_{ij} у гілках мережі визначається по методу Ерланга:

$$v_{ij} = \Psi(Z_{ij}, p_{ij}).$$

Етап 5. Корекція значень ймовірності втрат на гілках мережі

Кількість каналів, що розраховується, у гілках мережі може приймати лише дискретні, цілі значення. У зв'язку з цим у процесі розрахунку здійснюються округлення, як правило, убік збільшення числа необхідних каналів. Тому після визначення числа каналів у гілках мережі здійснюється уточнення величини втрат на гілках, що змінюється убік зменшення. Для одержання остаточного результату з заданою точністю необхідно по етапах 3, 4 і 5 виконати ітераційну процедуру повторення розрахунків. Як показує практика, число ітерацій у більшості випадків не перевищує двох-трьох.

Етап 6. Перевірочний розрахунок значень ймовірностей втрат і виконаного навантаження в напрямках зв'язку

Для перевірки відповідності виконання вимог по пропускній здатності здійснюється перевірочний розрахунок ймовірностей утрат у всіх чи основних напрямках зв'язку. З цією метою може використовуватися вираз (7). При збігу (із заданою точністю) результатів розрахунку з пропонованими вимогами уточнюється величина виконаного навантаження. Якщо результат перевірочного розрахунку незадовільний, зазначена вище ітераційна процедура цілком або частково повинна бути продовжена до одержання прийнятних результатів.

Порядок розрахунку живучості комутованої телекомунікаційній мережі

Як вже наголошувалося раніше, початковими даними для розрахунку живучості ТКМ є значення вірогідності виживання елементів мережі – гілок і комутаційних центрів. Процес розрахунку живучості має ряд загальних рис з розрахунком надійності.

Живучість ТКМ в цілому визначається живучістю її напрямів зв'язку. Показником живучості напрямів зв'язку W(J) є вірогідність збереження їх зв'язності. Якщо у напрямі зв'язку є тільки один шлях передачі інформації, що складається з послідовно включених гілок і комутаційних центрів, то живучість напряму зв'язку рівна живучості цього шляху W(μ) і визначається наступним виразом:

$$W(\mu)=\prod_{i=1}^{k-1} W_{mi} \prod_{j=1}^{k} W_{КЦj}, \qquad (8)$$

де W_{mi} – вірогідність виживання і – тій гілці;
$W_{КЦj}$ – вірогідність виживання j – того КЦ.

Якщо у напрямі зв'язку є (J) незалежних шляхів передачі інформації живучість напряму зв'язку визначається наступним виразом:

$$W(J)=1-\prod_{l=1}^{\chi(J)}\left[1-W\left(\mu_l\right)\right] \qquad (9)$$

З урахуванням (12) вираз (13) прийме наступний вигляд:

$$W(J)=1-\prod_{l=1}^{\chi(J)}\left[1-\prod_{i=1}^{k-1} W_{mil} \prod_{j=1}^{k} W_{КЦjl}\right]$$

Отже, порядок розрахунку живучості наступний:

1. Визначення початкових даних – вірогідності виживання гілок і КЦ.
2. Перетворення структури мережі в паралельно – послідовний граф
3. Складання розрахункового виразу і визначення показників живучості напрямів зв'язку.

Порядок розрахунку надійності функціонування комутованої телекомунікаційній мережі

Найбільш поширено два методи розрахунку – спрощений і диференційний. Точніший – диференційний. Ми користуватимемося спрощеним методом, оскільки він менш трудомісткий. Суть його полягає в тому, що спочатку визначається вірогідність безвідмовного обслуговування заявок на кожній гілці ТКМ:

$$W_m(t)=R_m(1-p_m), \qquad (10)$$

де R_m – вірогідність безвідмовної роботи гілки;
p_m – вірогідність втрат на гілці.

Для кожного напряму зв'язку відповідно до його складу створюється розрахунковий паралельно-послідовний граф. Кожному ребру графа присвоюється значення $W_m(t)$, визначене з використанням виразу (6). Використовуючи перетворення, здійснювані по методу імовірнісних графів, можна отримати вірогідність безвідмовного обслуговування в кожному напрямі зв'язку. Якщо напрям зв'язку J_{ij} складається з одного шляху передачі інформації, то вірогідність безвідмовного обслуговування $W_{ij}(t)$ у напрямі зв'язку визначається таким чином:

$$W_{ij}(t) = \prod_{r=1}^{k-1} W_{m_r}(t), \tag{11}$$

де W_{mr} – вірогідність безвідмовного обслуговування заявок в гілці m_r;
k – число КЦ в шляху передачі інформації.

Якщо напрям зв'язку складається з декількох незалежних шляхів передачі інформації, то вірогідність безвідмовного обслуговування у напрямі зв'язку визначається таким чином:

$$W_{ij}(t) = 1 - \prod_{g=1}^{\chi_{ij}} \left[1 - \prod_{r=1}^{k-1} W_{m_{rg}}(t) \right], \tag{12}$$

де χ – число незалежних шляхів в графі або напрямі зв'язку;
$W_{mrg}(t)$ – вірогідність безвідмовного обслуговування заявок в гілці m_{rg} .

Розглянемо сутність перетворень по методу імовірнісних графів, яка відображена на рис. 2.

На першому етапі непаралельно-послідовний граф перетворюється в паралельно-послідовний. Потім на його основі складаються розрахункові вирази для визначення чисельних значень вірогідності безвідмовного обслуговування в кожному напрямі зв'язку.

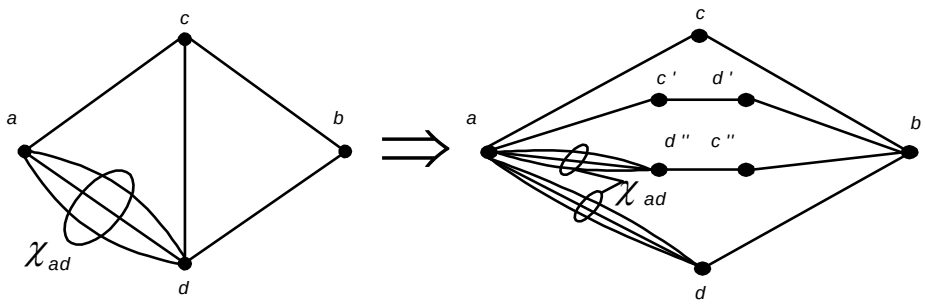


Рисунок 2.8 – Метод імовірнісних графів

Вірогідність безвідмовної роботи Rm гілок при використанні спрощеного методу визначається таким чином:

$$R_m = k_{гm} e^{-\frac{t}{T_m}}, \quad (13)$$

де $k_{гm}$ – коефіцієнт готовності гілки;
t – безперервний час виконання завдання;
T_m – середній час напрацювання на відмову.

Коефіцієнт готовності $k_{гm}$ визначається таким чином:

$$k_{гm} = T_m / T_m + T_{mв}, \quad (14)$$

де $T_{mв}$ – середній час відновлення пошкодженої гілки.

Враховуючи, що всі канали включені в гілці паралельно, отримуємо:

$$R_m = 1 - \prod_{i=1}^{\chi_m} (1 - R_{ni}), \quad (15)$$

де χ – число пучків, що утворюють гілку.

По розрахованих значеннях R_m визначаються значення $W_m(t)$ по виразу (10). Потім по виразах (11) або (12) визначається вірогідність безвідмовного обслуговування в кожному напрямі зв'язку.

2.3. Моделі та методи синтезу і аналізу телекомунікаційних мереж

2.3.1. Поняття про задачі синтезу та аналізу

Усі задачі, які виникають у процесі побудови та експлуатації телекомунікаційних мереж, можна розділити на два класи: задачі синтезу й аналізу зв'язаних мереж.

Під ***зв'язаною мережею*** розуміють сегмент телекомунікаційної мережі, для кожної пари пунктів якого може бути знайдено, принаймні, один шлях, який їх пов'язує.

Задача синтезу зв'язаної мережі постає як у процесі побудови нової мережі, так і під час реконструкції та розвитку наявних мереж. За типом ця задача є техніко-економічною, тому що найчастіше треба знайти рішення, оптимальне за економічними показниками, такими, наприклад, як мінімум капіталовкладень, максимум рентабельності та ін.

Для синтезу мережі, зазвичай, є заданим географічне розташування пунктів мережі, які слід об'єднати в зв'язну мережу (саме поняття "синтез" у перекладі з грецької означає "з'єднання", "складання"). При цьому топологія ліній зв'язку є невідомою характеристикою, яку необхідно з'ясувати, й вона

може варіюватися залежно від оптимізації економічних показників. Це дає змогу розглядати мінімум витрат на лінії зв'язку як цільовий критерій оптимального синтезу мережі.

На конфігурацію ліній зв'язку між пунктами мережі може бути накладено обмеження, зокрема заборона окремих географічних трас, наприклад, якщо вони перетинають водні або гірські перешкоди.

У класі задач аналізу розглядають питання визначення структурних характеристик як мережі в цілому, так і окремих її елементів. Конкретними задачами є такі, розв'язування яких – це вибір оптимальної топології фізичних зв'язків на певних ділянках мережі, підвищення надійності та живучості мережі, вибір оптимальної кількості й місця розташування вузлових пунктів та ін.

Задачі аналізу є актуальними для наявних, тобто вже синтезованих зв'язаних мереж. Такі задачі спрямовано на знаходження екстремальних шляхів передавання інформаційних потоків, визначення сукупності шляхів обмежених кількістю транзитів, оцінювання пропускної здатності мережі, ймовірності підтримання зв'язку між пунктами та ін.

Для того, щоб вирішити конкретне завдання синтезу або аналізу телекомунікаційної мережі, її необхідно ***формалізувати,*** тобто записати у вигляді схеми: що дано, що необхідно визначити і з якими обмеженнями.

Формалізацію можна виконати словесно (таку форму називають *вербальною моделлю* завдання) або у вигляді *математичної моделі,* яка описує завдання термінами тієї чи іншої теорії (наприклад, теорії графів, теорії множин, теорії оптимальних рішень та ін.)

Здійснення формалізації вимагає не тільки розуміння самої проблеми, а й вибору адекватної моделі об'єкта (телекомунікаційної мережі). Моделювання об'єкта синтезу або аналізу дає змогу з'ясувати та відтворити найбільш істотні, відповідно до поставленого завдання, елементи об'єкта та зв'язки між ними, не відволікаючись на деталі.

Для модельного відтворення зв'язаної мережі найчастотніше застосовують графи. На основі моделі об'єкта та її параметрів (кількості пунктів та ліній мережі, відстаней між пунктами, пропускної здатності вузлів і ліній мережі, вартісних параметрів та ін.) можна побудувати математичну модель, яка відображає залежність між параметрами, які відшукують, та незалежними змінними завдання.

У задачах синтезу та аналізу зв'язаних мереж найчастіше використовують ***оптимізаційні математичні моделі,*** де критерій оптимізації записують як ***цільову функцію,*** для якої необхідно знайти ***екстремум*** (мінімум або максимум). На вхідні в цільову функцію параметри, як правило, накладають обмеження, які вказують, у яких межах можуть змінюватися значення параметрів, які відшукують. Обмеження записують як рівняння та нерівності, що містять деякі логічно пов'язані сукупності цих параметрів. Таку систему рівнянь або нерівностей називають системою обмежень задачі.

Задачі, в яких треба відшукати екстремум (мінімум або максимум) деякої цільової функції, що відображає критерій оптимальності рішення, називають ***екстремальними.***

Прикметною особливістю екстремальних задач синтезу та аналізу телекомунікаційних мереж є їх велика розмірність. Формулювання цих завдань термінами графових та мережних моделей дає змогу отримати значну кількість ефективних (зважаючи на подолання обчислювальної складності) методів та алгоритмів їх вирішення, орієнтованих на застосування ЕОМ. Такі алгоритми розглядатимемо далі.

Під ***алгоритмом*** розуміють формалізовану покрокову процедуру, що забезпечує знаходження рішення завдання, виконання якого можна доручити ЕОМ.

Розрізняють алгоритми *точні* та наближені, так звані *евристичні.*

Точні алгоритми завжди гарантують знаходження оптимального рішення (глобального оптимуму цільової функції). Наприклад, алгоритм повного перебору всіх можливих рішень з вибором найкращого серед них, є точним алгоритмом.

Точні алгоритми, як правило, досить трудомісткі. Тому у практиці часто використовують більш прості алгоритми, що забезпечують швидке вирішення з прийнятною точністю. Такі алгоритми будують, використовуючи раціональні, з точки зору логіки людини, *правила знаходження рішення.* Ці правила називають ***евристиками.*** Розв'язування задачі можна повторити, використовуючи інші евристики. Як доводить практика, збільшуючи витрати часу, ***евристичний алгоритм*** дає змогу знайти рішення, близьке до оптимального.

Евристичні алгоритми використовують у тих випадках, коли побудувати точний алгоритм не вдається через складність математичної моделі задачі (її нелінійність, дискретність та ін.).

Нагадаємо, що питання моделювання мереж були розглянуті нами у 1-ій та 2-ій темах навчальної дисципліни. Зокрема були введені поняття моделей телекомунікаційних мереж у вигляді:

– ***графа або*** сукупності розосереджених у просторі N пунктів (вузлів) і M ліній, які їх з'єднують;

– *матриці суміжності* розміром N×N, елементи якої приймають значення "1", якщо між відповідними вузлами є лінія зв'язку, або "0" – у протилежному випадку;

– ***матриці інцидентності*** розміром M×N, елементи якої приймають значення "1", якщо відповідна лінія зв'язку прилягає до певного вузла, або "0" – у протилежному випадку.

2.3.2. Задачі синтезу телекомунікаційних мереж

Розв'язування будь-якої задачі синтезу телекомунікаційної мережі обов'язково складатиметься з визначення топології фізичних зв'язків (проводових або безпроводових) для деякої заданої сукупності пунктів,

розосереджених у просторі. Неважко уявити, що кількість топологічних варіантів можливих фізичних зв'язків у цьому випадку, може бути доволі значною величиною. Закономірно постає питання про вибір такого варіанту, який відповідатиме деякому заздалегідь визначеному критерію оптимальності. Таким чином, можна констатувати, що задачі синтезу зв'язаних мереж є екстремальними, для вирішення яких, як вже зазначалося, можна застосовувати точні та евристичні алгоритми. Чим більшою є розмірність мережі, тим складнішим є застосування точних методів і алгоритмів.

Однак сегментний підхід у побудові телекомунікаційних мереж, дає змогу здійснювати декомпозицію загальної задачі синтезу мережі на ряд підзадач оптимального синтезу її сегментів, які виконують відносно самостійні завдання щодо забезпечення основної телекомунікаційної функції – транспортування інформаційних потоків. Отже, можна говорити про оптимальний синтез мережі абонентського доступу, транспортної мережі та ін.

Сучасна теорія графів пропонує витончені методи та алгоритми рішення завдань оптимального синтезу топологій фізичних зв'язків для сегментів телекомунікаційних мереж. Ось деякі з них:

Синтез зв'язаної мережі мінімальної вартості

Ситуація, в якій деяку множину точок необхідно поєднати так, щоб кожна пара точок стала зв'язною (безпосередньо або через інші точки), а загальна вагова характеристика зв'язків виявилася мінімальною, спонукає до **розв'язування** задачі синтезу мережі мінімальної вартості.

Наприклад, є ряд точок, у яких можуть бути розташовані пункти телекомунікаційної мережі. Відомо: відстані між парами точок і вартість прокладання одного кілометра лінії зв'язку. Необхідно визначити сукупність ліній зв'язку, які забезпечують зв'язність усіх пунктів мережі й мінімальну сумарну вартість їх прокладки.

З теорії графів і мереж відомо, що рішенням поставленого завдання є мережа з топологією фізичних зв'язків типу "дерево", тобто такого графа, в якому відсутні *цикли.*

Кажуть, що граф містить ***цикли,*** якщо в ньому можна відшукати замкнуті контури. Відсутність циклів визначає особливість графа типу "дерево", яка полягає в тому, що між будь-якою парою його вершин існує лише один єдиний шлях їх сполучення, тобто параметр зв'язності *h=1*. Кількість ребер (M) у дереві є завжди на одиницю меншою від кількості його вершин (N): N–M=1.

Означення. Граф типу "дерево" в якому для кожної пари вершин існує шлях, який їх з'єднує, називають ***покривним деревом*.**

Математично задача синтезу мережі мінімальної вартості зводиться до знаходження ***мінімального покривного дерева.*** Цю задачу формулюють наступним чином.

Нехай задано неорієнтований граф *G(N,M),* де множині вершин *N* відповідає множина пунктів мережі, загальне число яких дорівнює *n*, а множина ребер *M* – відстаням m_{ij} між парами пунктів.

Відома вартість C_{ij} організації одиниці довжини (наприклад, одного кілометра) лінії зв'язку між пунктами *i* та *j*.

Необхідно знайти деяке покривне дерево *G′(N,M′),* для якого досягається мінімум цільової функції:

$$z = \sum_{i=1}^{n} \sum_{j=1}^{n} C_{ij} m_{ij} \rightarrow min.$$

Для вирішення поставленої задачі існує ряд ефективних алгоритмів знаходження покривного дерева. Наведемо один із них, відомий за прізвищем автора як ***алгоритм Пріма.***

Алгоритм Пріма можна реалізувати шляхом надання позначок вершинам, які вводяться в відшукуваний граф *G′(N,M′),* і послідовного введення в нього мінімальних за вагою ребер. При цьому, як зазначено вище, загальна кількість ребер не повинна перевищувати (*n*–1) і між усіма *n* вершинами покривного дерева має бути зв'язність.

Процедуру виконання алгоритму Пріма у покроковій формі докладно розглянемо на наступному занятті.

Знаходження мінімального покривного дерева є однією з класичних задач оптимізації на графах і мережах, оригінальні розв'язування якої запропоновано багатьма авторами. Так, не менш відомим і, до того ж, більш ефективним, з урахуванням швидкості обчислень, є алгоритм, запропонований Краскелом.

Алгоритм Краскела відрізняється тим, що ребра в ньому проглядають у порядку зростання ваг і лиш одноразово. Звісно, це передбачає виконання попередньої процедури впорядкування ребер у порядку збільшення їх вагових характеристик. У разі однакових ваг ребра розташовують довільно.

Ідея алгоритму ґрунтується на процесі *"фарбування"* ребер і формуванні *"букетів"* із вершин. Пояснимо цю ідею.

Для фарбування ребер, які формуватимуть мінімальне покривне дерево, використовуємо, наприклад, блакитний колір, а для тих, що поза ним – жовтий. Якщо чергове незабарвлене ребро, взяте з упорядкованого списку, *не утворює цикл* з ребрами блакитного кольору, його забарвлюємо у блакитний колір, а з його вершини утворюємо "букет" вершин мінімального покривного дерева, яке будується. Інакше – ребро забарвлюємо у жовтий колір. Ребро може утворювати цикл у мінімальному покривному дереві лише в тому випадку, коли його вершини належать до одного "букету". Якщо ж вершини належать різним "букетам", то ребро забарвлюють в блакитний колір, а "букети" зливаються.

Процедуру завершують, коли кількість блакитних ребер досягає (*n*–1), або коли всі ребра будуть, не зважаючи на колір, пофарбованими. Процедуру

виконання алгоритму Краскела у покроковій формі так саме розглянемо на наступному занятті.

Визначення оптимального місця розташування опорного вузла в кабельній мережі абонентського доступу

Розглянемо наступне завдання. Нехай граф *G*(*N, M)* відображає деяку зв'язану мережу, тотожну кабельній мережі абонентського доступу, яка охоплює *n* абонентських пунктів. Вага кожного ребра *(i, j*), яке належить *M,* відповідає довжині m_{ij} або вартості прокладки кабелю, котрий з'єднує пункти *i* та *j*. Необхідно визначити деяку вершину n_i, що належить *N,* у якій доцільно розмістити опорний вузол (наприклад, районну АТС) з урахуванням мінімізації загальної довжини кабелю, який з'єднує абонентські пункти з опорним вузлом.

Рішенням поставленого завдання є визначення ***медіани графа G (N, M).***

Означення. Вершина n_i, яка належить N, є **медіаною** графа ***G (N, M)***, якщо вона не суперечить умові:

$$\sum_{j=1}^{n} m_{ij} \le \sum_{j=1}^{n} m_{kj}\,; \quad k \ne i.$$

Величину

$$R_{min} = \sum_{j=1}^{n} m_{ij}$$

називають ***медіанною довжиною*** графа *G,* вона є найменшою сумарною довжиною ребер, які з'єднують вершину n_i з іншими вершинами графа.

Покроковий алгоритм визначення медіани графа *G* розглянемо на наступному занятті.

Визначення оптимального місця розташування базової станції в мережі стаціонарного радіодоступу

Припустимо, що задано розташування пунктів мережі, в якій реалізовано абонентський стаціонарний радіодоступ до базової станції (БС). Необхідно знайти місце розташування базової станції, яка по радіоканалах зв'язується з абонентськими пунктами (АП). Бажано, щоб відстань від БС до будь-якого АП була мінімальною, що забезпечить стійкий радіозв'язок з урахуванням меншої потужності передавача БС. Зрозуміло, що такий критерій задовольнити майже неможливо. Тому будемо мінімізувати відстань до найбільш віддаленого від БС абонентського пункту, решта АП в цьому випадку автоматично буде знаходиться ближче до БС. Закономірно, що БС (якщо це можливо) повинна займати центральне положення відносно всіх АП.

Задача знаходження пункту, в якому доцільно розташувати БС, може бути зведена до задачі знаходження ***центра графа.***

Означення. Нехай $G(N,M)$ є графом, де N – множина вершин, а L – множина відстаней між усіма вершинами. Вершину ***s*** називають центром графа $G(N,M)$, якщо вона не суперечить умові:

$$max\ m_{sj} \le max\ m_{ij} \text{ для будь-якої } i;\ 1 < j < N.$$

Алгоритм знаходження центра графа (вершини *s*) випливає з самого визначення. Покрокову процедуру розглянемо на наступному занятті.

Визначення циклу найменшої довжини для організації транспортного кільця

Кільцеві топології фізичних зв'язків, як випливає з попередніх розділів, часто використовують для побудови сегментів телекомунікаційних мереж, особливо транспортних мереж.

У термінах теорії графів кільцеву топологію визначають як ***цикл*** або ***контур.*** Під ***циклом*** розуміють послідовність дуг (ребер) графа, що складають шлях, який починається й закінчується в одній і тій же вершині, а під ***контуром*** – послідовність вершин графа, які входять у такий цикл.

Пошук циклу (контуру) є доцільний лише в „надлишковому" відносно деревоподібного графа, тобто в графі, кількість ребер якого є більшою від числа *n* його вершин. Власне кажучи, в задачах синтезу в такому сенсі вихідний граф допустимих зв'язків між вершинами завжди є надлишковим. У такому графі можна утворити $n!$ циклів, які містять дуги (ребра) різної ваги, серед яких можна відшукати цикл найменшої сумарної ваги дуг (ребер). Розв'язавши подібну задачу можна, наприклад, оптимізувати витрати на побудову транспортної мережі.

Задача про знаходження циклу найменшої довжини в теорії графів є відомою як ***„задача комівояжера".*** Вона може бути формалізована наступним чином.

Дано граф *G(N,M),* вершини якого – це міста в зоні обслуговування комівояжера, а дуги – відповідно зв'язки між парами міст. Маршрутом комівояжера називається контур, який містить всі вершини графа *G*. Необхідно знайти маршрут найменшої довжини.

Розв'язком цієї задачі є ***гамільтонов контур*** в графі *G(N,M)*, який відповідає маршруту найменшої довжини. Назва „гамільтонов контур" походить від прізвища ірландського математика Вільяма Гамільтона, який у 1859 року вперше розпочав дослідження цих задач.

Означення. Контур, у якому розміщено кожну вершину графа *G(N,M)* тільки один раз, називають ***гамільтоновим контуром*** (або гамільтоновим циклом).

Задачу про знаходження гамільтонового контуру можна розв'язати за допомогою точного методу або евристичного більш докладно розглянемо їх на наступному занятті.

2.3.3. Задачі аналізу телекомунікаційних мереж

Задачі аналізу телекомунікаційної мережі, як уже зазначено вище, ґрунтуються на синтезованої топології фізичних зв'язків, і найчастіше зводяться до з'ясування оптимальних топологій логічних зв'язків. Це стосується побудови оптимальних планів розподілу інформаційних потоків у мережі, вибору найкращих маршрутів передавання інформаційних повідомлень, підвищення надійності та живучості мережі та ін.

Задачі синтезу та аналізу дуже пов'язані між собою, оскільки можливості оптимізації топології логічних зв'язків обмежуються топологією фізичних зв'язків у мережі. Якщо неможливо виконати умови оптимальної побудови топології логічних зв'язків, доводиться повертатися до синтезу інших топологій фізичних зв'язків. У результаті побудова телекомунікаційної мережі та її сегментів перетворюється на ітераційний процес.

Нижче розглядаємо окремі класичні задачі аналізу зв'язаних мереж, що засновані на графових моделях.

Знаходження найкоротшого шляху в зв'язаній мережі

Задача про знаходження найкоротшого за довжиною шляху в зв'язаній мережі є фундаментальною задачею комбінаторної оптимізації. За її допомогою можна вирішити широке коло практичних завдань, які виникають у процесі керування телекомунікаційними мережами, впровадження нових телекомунікаційних технологій, методів маршрутизації та ін. Закономірно, що як „довжини" можуть розглядатися будь-які інші вагові характеристики елементів графа.

Означення. ***Шляхом*** називають послідовність вершин $\mu_{ij} = (i, r, \ldots, j)$ або послідовність дуг (ребер) $\mu_{ij} = \{(i, r), \ldots, (k, j)\}$, що з'єднують пару i та j вершин графа G.

Сума ваг, приписаних дугам (ребрам), які утворюють шлях μ_{ij}, визначає його ***довжину.***

Шлях з вершини i в вершину j, який має мінімально можливу довжину, є ***найкоротшим шляхом.***

Задачу про знаходження найкоротшого шляху можна сформулювати в наступному вигляді. Дано зв'язану мережу G, у якій кожній дузі (ребру) приписано вагу, пропорційну до її (його) довжини. Потрібно знайти шлях μ_{st} між заданими вершинами s та t, який має мінімально можливу довжину, тобто

$$l = \sum_{(i,j)\in\mu_{st}} m_{ij} \rightarrow \min(\text{на } \mu')$$

де μ' – множина всіх можливих шляхів з s до t.

Найбільш ефективними алгоритмами, які вирішують поставлене завдання, є ***алгоритми Дейкстри та Белмана-Форда.***

Алгоритм Белмана-Форда

Нехай вузол 1 є вузлом-джерелом і треба знайти довжини найкоротших шляхів від нього до кожного іншого вузла мережі (графа). Для цього алгоритму дугові відстані можуть бути як позитивними, так і негативним, але ми припустимо, що немає циклів від'ємної довжини (це припущення буде обговорено далі детальніше). Для спрощення позначень положимо $a_{ij} = \infty$ якщо в графі відсутня дуга (***i***, ***j***). Основна ідея алгоритму Белмана-Форда полягає в тому, щоб спочатку знайти довжини найкоротших шляхів за умови, що шляхи мають не більше однієї дуги, потім довжини найкоротших шляхів, за умовою, що шляхи мають не більше двох дуг і т.д. Найкоротший шлях за умови, що шлях має не більше ***h*** дуг, в подальшому буде називатися найкоротшим ($\leq h$) шляхом.

Нехай $\mathbf{D}_i^{(h)}$ – довжина найкоротшого ($\leq h$) шляху від вузла 1 до вузла ***i***. Будемо вважати, що $\mathbf{D}_i^{(h)} = 0$ для всіх ***h***. Алгоритм Белмана-Форда полягає в наступному. Спочатку

$$D_i^{(0)} = \infty \qquad \text{для всіх } i \neq 1.$$

При кожному наступному $h \geq 0$

$$D_i^{(h+1)} = \min\left[D_i^{(h)} + d_{ij}\right] \qquad \text{для всіх } i \neq 1.$$

Для доведення того, що цей алгоритм приводить до правильного рішення, помітимо спочатку, що (1) і (2) дають $\mathbf{D}_i^{(1)} = d_{ij}$ – для всіх $i \neq 1$ і вони дійсно є довжинами найкоротших (≤ 1) шляхів. Далі проведемо доведення індукцією по ***h***, вважаючи для даного ***h***, що $\mathbf{D}_i^{(h)}$ є довжинами найкоротших ($\leq h$) шляхів для всіх $i \neq 1$, і доводячи, рівність (2) дає довжину найкоротшого ($\leq h + 1$) шляху від вузла 1 до кожного вузла $i \neq 1$. Спочатку покажемо, що ліва частина (2) більша чи рівна правої частини, а потім доведемо протилежну нерівність. Припустимо, що (1, ... , ***m***, ***к***, ***i***) – найкоротший ($\leq h + 1$) шлях від 1 до ***i***. Тоді його довжина дорівнює довжині шляху (1, ..., ***m***, ***к***, ***i***). Так як (1,…, ***m***, ***к***, ***i***) має не більше *h* дуг, то

$$D_i^{(h+1)} \geq D_k^{(h)} + d_{ki} \geq \min_j \left[D_j^{(h)} + d_{ji} \right]$$

Для доведення оберненої нерівності припустимо, що мінімум в правій частині (2) досягається при $j = k$ і що (1,...,***m***, ***k***) є найкоротшим ($\leq h$) шляхом, довжина якого за припущенням рівна $\mathbf{D}_к^{(h)}$. Тоді довжина шляху (1,...,***m***, ***k***, ***i***) рівна правій частині (2). Тому якщо (1,..., ***m***, ***k***, ***i***) – деякий шлях, то

$$D_i^{(h+1)} \leq D_k^{(h)} + d_{ki} \geq \min_j \left[D_j^{(h)} + d_{ji} \right].$$

$$D_i = \min_j \left[D_j + d_{ji} \right] \qquad \text{для всіх } i \neq 1.$$

$$\mathbf{D}_1 = 0$$

Це **рівняння Белмана**, воно означає, що довжина найкоротшого шляху від вузла 1 до *i* дорівнює сумі довжини шляху до вузла, який передує вузлу ***i*** (на найкоротшого шляху) і відстані на останній дузі шляху. Із розв'язку цього рівняння (яке можна отримати використовуючи алгоритм Белмана-Форда) легко знайти найкоротші шляхи (а не довжини найкоротших шляхів), враховуючи, що всі цикли, які не включають вузол 1, мають додатну довжину. Щоб це зробити треба відібрати для кожного $\boldsymbol{i} \neq 1$ по одній дузі (***i, j***), на якій досягається мінімум в (3), і розглянути підграф, який складається з відібраних (**N**-1) дуг.

Використовуючи попередню конструкцію, можна довести, що *якщо немає циклів нульової* (*або від'ємної*) *довжини, то рівняння Белмана* (3) *має єдиний розв'язок.*

Відмітимо, що популярність алгоритму Беллмана-Форда пояснюється тим, що у випадку, коли довжини всіх дуг додатні, початкові умови $\mathbf{D}_i^{(0)}$ для $\boldsymbol{i} \neq 1$ можуть бути будь-якими невід'ємними числами і ітерації (2) можуть виконуватися паралельно для різних вузлів в довільному порядку, що має велике значення для додатків з розподіленими алгоритмами.

Алгоритм на кожному кроці перевіряє всі варіанти можливих шляхів, що призводить до значного зростання обчислювальної складності.

Алгоритм припиняє свою роботу тільки у відповідності з адміністративними обмеженнями, в іншому випадку алгоритм працює нескінченно намагаючись знайти кращий шлях до потрібного вузла.

Алгоритм маршрутизації Дейкстри

Цей алгоритм потребує, щоб довжини всіх дуг були додатніми (ця умова виконується у всіх мережах передачі даних). Об'єм обчислень зростає в гіршому випадку для цього алгоритму значно повільніше, ніж у алгоритму Белмана-Форда. Основна ідея алгоритму полягає в тому, щоб відшуковувати найкоротші шляхи в порядку зростання довжини шляху. Найкоротшим серед усіх найкоротших шляхів від вузла **1** є шлях, який складається з однієї дуги, яка з'єднує вузол **1** з найближчим сусіднім вузлом, так як будь-який шлях, що складається з кількох дуг, буде завжди довшим ніж довжина дуги внаслідок припущення про додатність усіх дугових довжин. Наступним найкоротшим серед найкоротших шляхів повинен бути або шлях із однієї дуги до наступного найближчого сусіда вузла **1**, або найкоротший шлях з двох дуг, який проходить через вузол вибраний на першому кроці і т.д.

Щоб формально описати цю процедуру у вигляді алгоритму, будемо вважати що кожен вузол ***i*** має мітку $\mathbf{D}_i$, що позначає оцінку довжини найкоротшого шляху від вузла **1.** Коли оцінка стає незмінною, будемо рахувати, що вузол ***поміченій***, і множину остаточно помічених вузлів позначимо через **P**. Вузол, котрий буде доданий на черговому кроці до **P**, є найближчим до вузла **1** серед усіх вузлів, які ще не увійшли в **P**.

Особливістю цього алгоритму є те, що в процесі його виконання одночасно будують найкоротші шляхи з заданої вершини *s* до усіх інших вершин мережі. Це пояснюється тим, що будь-яка вершина *i* є *N* може виявитися проміжною на найкоротшому шляху з *s* до *t*. Після закінчення роботи алгоритму вершина *s* стає з'єднаною з усіма іншими вершинами зв'язаної мережі *G*, зокрема і з вершиною *t*, найкоротшими шляхами, а дуги (ребра), які увійшли до них, утворюють деяку підмережу без циклів, тобто "дерево" з коренем у вершині *s*.

З початку $\mathbf{P} = \{1\}$, $\mathbf{D}_1 = 0$ і $\mathbf{D}_j = \boldsymbol{d}_{1j}$ для $\boldsymbol{j} \neq 1$.

Крок 1 (пошук наступного найближчого вузла). Знайти $\boldsymbol{i} \notin \mathbf{P}$, такий, що

$$D_i = \min_{j \neq p} D_j$$

Покласти $\mathbf{P} := \mathbf{P} \cup \{\boldsymbol{i}\}$. Якщо **P** містить всі вузли, то на цьому робота алгоритму закінчується.

Крок 2 (відновлення міток). Для всіх $\boldsymbol{j} \notin \mathbf{P}$ покласти

$$D_i := \min \left[D_j, D_i + d_{ji} \right]$$

Перейти до кроку 1.

Робота алгоритму реалізується за допомогою розміщення у вершинах позначок (L_{sj}, i), де L_{sj} – довжина найкоротшого шляху з початкової вершини *s* до деякої вершини *j*, а *i* попередня до *j* – вершина на цьому шляху.

Позначки поділяють на *тимчасові* та *постійні.* Тимчасові позначки можуть змінюватися в результаті роботи алгоритму, а постійні – не змінюються.

Алгоритм Дейкстри припиняє роботу, як тільки всі вершини стають позначеними.

Крок 0. Для вершини *s* вважатиме, що $L_{ss} = 0$, а для решти вершин $L_{sj} = \infty$. Усі вершини мають тимчасові позначки типу (L_{sj}, s).

Трасування шляху μ_{st} здійснюється у зворотному напрямку, прямуючи з вершини *t* до *s*, керуючись вершинами *i* в постійних позначках.

Основна ідея алгоритму Дійкстри полягає в тому, щоб відшуковуватн найкоротші шляхи в порядку зростання довжини шляху.

Визначення множини шляхів заданої кількості транзитів

Серед обмежень, які накладаються у процесі знаходженні шляхів у зв'язаних мережах, можна розглядати обмеження на їх транзитність.

Під ***транзитністю шляху*** μ_{st} розуміють кількість проміжних пунктів, які входять до нього (без урахування початкового *s* і кінцевого *t* пунктів), або кількість ліній зв'язку, які з'єднують на шляху тільки транзитні пункти. Кількість проміжних пунктів називають ***параметром транзитності T*** на шляху μ_{st}.

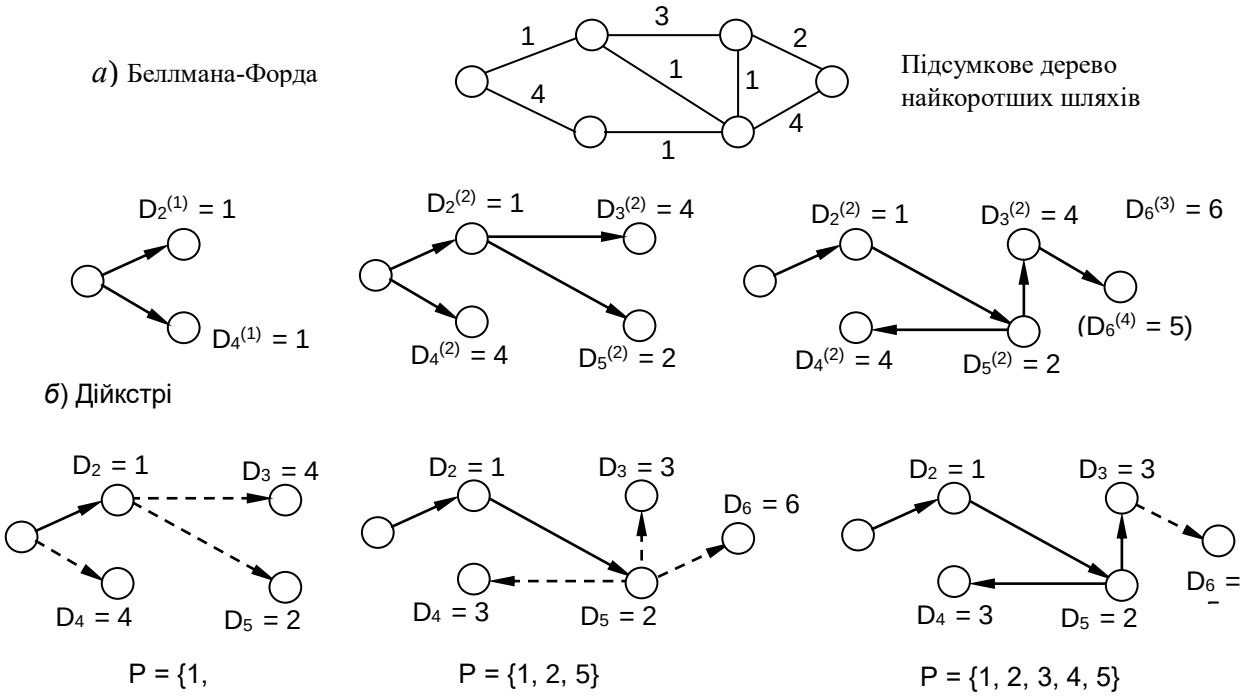


Рисунок 2.9 – Визначення найкоротшого шляху за алгоритмом Беллмана-Форда і Дійкстри

Обмеження за транзитністю на шляху надсилання повідомлення залежать від вимог до якості обслуговування у мережі (наприклад, до часу проходження повідомлення мережею, часу оброблювання повідомлення у вузлах та ін.).

Термінами теорії графів завдання формулюємо таким чином.

Дано деякий вихідний граф *G(N, M),* необхідно визначити множину шляхів $\mu'=\{\mu_{si}\}$ із заданої вершини *s* до інших вершин $i \in N,\ i \neq s,\ i = 1, ..., n$, графа *G*, для яких параметр транзитності *T* не перевищує певної заданої величини T_0, тобто

$$T \leq T_0, \forall\, \mu_{si}, i \neq s, i = 1 \ldots n.$$

Одним з найбільш зручних і легких для реалізації на ЕОМ методів визначення шляхів, які відповідають цій вимозі, є побудова так званого ***"ярусного дерева"*** шляхів від заданої вершини *s* до інших вершин графа.

На рисунку 2.10 наведено вихідний граф та відповідне йому „ярусне дерево" з параметром $T_0 = 2$.

Алгоритми знаходження екстремальних шляхів (найкоротших за довжині, за транзитністю) застосовують для визначення оптимальних маршрутів як у мережах із пакетною комутацією, так і в мережах із комутацією каналів. Результати їх роботи, зазвичай, зводять до побудови маршрутних матриць, які зберігаються в транзитних пунктах телекомунікаційних сегментів із комутованої топологією. Вони призначені

для визначення вихідного порту під час комутації вхід – вихід, наприклад, у маршрутизаторах, комутаційних телефонних станціях.

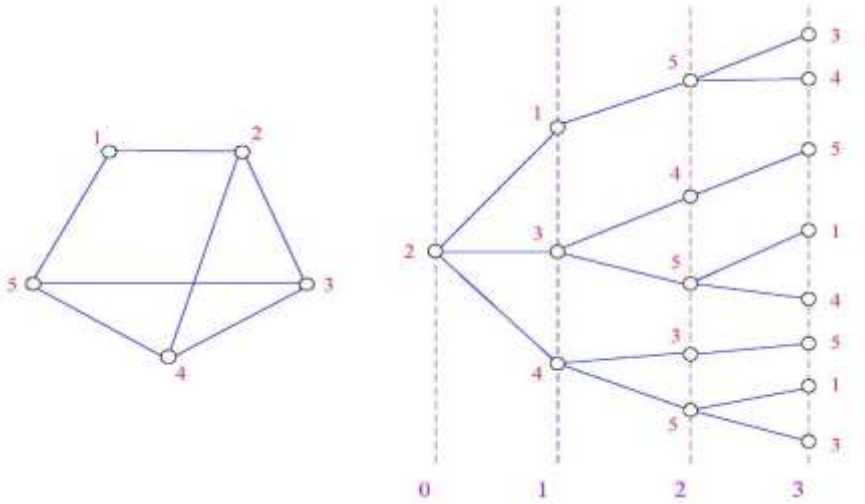


Рисунок 2.10 – Ілюстрація роботи алгоритму побудови ярусного дерева

Контрольні питання до розділу 2

1. Якість обслуговування в телекомунікаційних мережах (властивості, сутність QoS, складові, приклади показників).
2. Живучість телекомунікаційних мереж (визначення, сутність, одиниці виміру, спосіб розрахунку).
3. Поясніть зміст та порядок роботи алгоритму Дейкстри.
4. Описати порядок постановки і рішення задачі визначення оптимального місця розташування базової станції в мережі стаціонарного радіодоступу.
5. Описати порядок постановки і рішення задачі визначення можливих шляхів із заданим показником транзитності.

РОЗДІЛ 3
ПРИНЦИПИ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНИХ ТА ІНФОРМАЦІЙНИХ МЕРЕЖ І КЕРУВАННЯ НИМИ

3.1. Принципи, технології та обладнання комутації

3.1.1. Принципи комутації

Комутація є необхідним елементом зв'язку вузлів між собою, що дозволяє скоротити кількість необхідних ліній зв'язку і підвищити завантаження каналів зв'язку. Практично неможливо надати кожній парі вузлів виділену лінію зв'язку, тому в мережах завжди застосовується той або інший **спосіб комутації абонентів**, що використовує існуючі лінії зв'язку для передачі даних різних вузлів.

Для локальних мереж застосовують **комутацію пакетів** (всі передані користувачем дані розбиваються передавальним вузлом на невеликі частини - **пакети** (кадри)). Кожен пакет оснащується заголовком, в якому вказується, як мінімум, адреса вузла-одержувача та номер пакету. Передача пакетів по мережі відбувається незалежно один від одного. Комутатори такої мережі мають внутрішню буферну пам'ять для тимчасового зберігання пакетів, що дозволяє згладжувати пульсації трафіка на лініях зв'язку між комутаторами.

Комутатор LAN підтримує таблицю, за допомогою якої визначає, як пересилати трафік через комутатор. Ця таблиця зберігається в асоціативній пам'яті (CAM – Content-addressable memory), яка є особливим типом пам'яті, що використовується у високошвидкісних пошукових застосунках. З цієї причини таблиця MAC-адрес іноді називається CAM-таблицею. Комутатор пересилає трафік на основі номеру вхідного порту і MAC-адреси призначення кадру.

Комутатор складається з інтегральних мікросхем та супутнього програмного забезпечення, яке контролює шляхи передавання даних через комутатор.

Щоб комутатор знав, який інтерфейс використовувати для передавання кадру, спочатку потрібно дізнатись, які пристрої підключені з боку кожного інтерфейсу. При надходженні кожного кадру Ethernet на комутатор виконується такий двоетапний процес.

Крок 1. Навчання – вивчення MAC-адреси джерела

При отриманні кожного кадру комутатор перевіряє його на наявність нової інформації. Для цього перевіряється MAC-адреса джерела кадру та номер інтерфейсу, через який кадр надійшов до комутатора.

- Якщо у таблиці MAC-адрес немає MAC-адреси джерела, ii та відповідний номер вхідного інтерфейсу додають до таблиці.
- Якщо MAC-адреса джерела вже існує, комутатор оновлює таймер оновлення для цього запису.

За замовчуванням більшість комутаторів зберігають запис у таблиці протягом п’яти хвилин. Якщо MAC-адреса джерела присутня в таблиці, але на іншому інтерфейсу, комутатор розглядає це як новий запис.

Крок 2. Пересилання – перевірка MAC-адреси призначення

Якщо MAC-адреса призначення є адресою індивідуальної розсилки, комутатор буде шукати відповідність між MAC-адресою призначення кадру та записом у його таблиці MAC-адрес:

- Якщо MAC-адреса призначення наявна в таблиці, комутатор передасть кадр через визначений інтерфейс.
- Якщо MAC-адреса призначення відсутня у таблиці, комутатор передасть кадр через усі інтерфейси за винятком вхідного інтерфейсу. Це називається індивідуальна розсилка невідомому отримувачу (unknown unicast).

Якщо MAC-адреса призначення є широкомовною або адресою групової розсилки, кадр також передається через усі інтерфейси, крім вхідного інтерфейсу.

У сегментах Ethernet на основі *концентратора* мережні пристрої змагалися за спільне середовище. Сегменти мережі, в яких пристрої спільно можуть використовувати смугу пропускання, називаються ***доменами колізій***. Якщо два або більше пристроїв в одному домені колізій одночасно намагаються передавати дані, виникає ***колізія*** – накладання двох та більше кадрів від станцій, що намагаються передати кадр в один і той же момент часу.

У сегментах Ethernet на основі *комутатора* можливість виникнення колізій визначається режимом роботи інтерфейсів комутатора. Коли інтерфейси комутатора працюють у повнодуплексному режимі, доменів колізій не існує. Якщо комутаційний інтерфейс Ethernet працює у напівдуплексному режимі, кожен сегмент перебуває у своєму власному домені колізій.

За замовчуванням інтерфейси комутатора Ethernet мають повнодуплексний режим, якщо суміжний пристрій може також може у ньому працювати, а також найвищу пропускну здатність, доступну для обох пристроїв. Якщо інтерфейс комутатора під’єднаний до такого пристрою, як традиційний концентратор, що працює у напівдуплексному режимі, цей інтерфейс працюватиме в напівдуплексному режимі. У такому випадку, комутаційний інтерфейс буде частиною домену колізій.

Сукупність з’єднаних між собою комутаторів формує єдиний ***широкомовний домен***, до нього належать усі пристрої локальної мережі, які отримують кадри широкомовної розсилки від вузла. Коли комутатор отримує широкомовний кадр, він пересилає кадр з усіх своїх інтерфейсів, за винятком вхідного інтерфейсу, на якому широкомовний кадр був отриманий. Кожен пристрій, під’єднаний до комутатора, отримує копію широкомовного кадру і обробляє її. Тільки пристрій мережного рівня, наприклад, маршрутизатор, здатен розділити широкомовний домен Рівня 2. Маршрутизатори

використовуються для сегментації доменів широкомовної розсилки, але вони також відокремлюють домени колізій.

3.1.2. Протоколи та технології комутації

Комутатори дуже швидко приймають рішення щодо переадресації Рівня 2. Це пов'язано з програмним забезпеченням на спеціалізованих інтегральних схемах (ASIC – application-specific integrated circuit). ASICs скорочують час оброблення кадрів на пристрої і дозволяють пристрою керувати збільшеним числом кадрів без зниження продуктивності.

Комутатори Рівня 2 використовують один із двох способів комутації кадрів:

- **Метод комутації з проміжним збереженням (Store-and-forward switching)** – при використанні цього методу рішення про переадресацію кадру приймається після отримання повного кадру і його перевірки на наявність помилок за допомогою математичного механізму – циклічного надлишкового коду (CRC). Комутація з проміжним збереженням є основним методом комутації локальної мережі Cisco.
- **Метод наскрізної комутації (Cut-through switching)** – при наскрізний комутації процес пересилання починається після визначення MAC-адреси призначення вхідного кадру і вихідного інтерфейсу.

На відміну від наскрізної комутації, комутація із проміжним збереженням має такі дві основні особливості:

- **Перевірка помилок** – після отримання всього кадру комутатор порівнює значення перевірочної послідовності кадру (FCS), наведене в останньому полі, з власними розрахунками FCS. FCS – це процес виявлення помилок, який дозволяє переконатися в тому, що кадр не містить фізичних і канальних помилок. Якщо проблем не виявлено, комутатор пересилає кадр, в іншому випадку кадр відкидається.
- **Автоматична буферизація** – процес буферизації на вхідному інтерфейсу, який використовується комутаторами з проміжним збереженням, забезпечує гнучкість для підтримки будь-яких швидкостей Ethernet.

Наприклад, обробка вхідного кадру, що передається через інтерфейс Ethernet 100 Мбіт/с і призначеного для відправки на інтерфейс 1 Гбіт/с, зажадає використання комутації з проміжним збереженням. З будь-якою невідповідністю у швидкості між вхідним і вихідним інтерфейсами комутатор зберігає весь кадр у буфері, перевіряє FCS, пересилає його в буфер вихідного інтерфейсу і потім відправляє його.

На рисунку 3.1 показано, як комутація з проміжним збереженням приймає рішення на основі кадру Ethernet.

Метод комутації з проміжним збереженням видаляє кадри, які не проходять перевірку FCS. Таким чином, він не пересилає неприпустимі (помилкові) кадри. І навпаки, в режимі наскрізної комутації можливе пересилання невідповідних кадрів, оскільки перевірка FCS не виконується. У разі високого коефіцієнта помилок (неприпустимих кадрів) у мережі,

наскрізна комутація може негативно позначитися на пропускній здатності, наповнюючи її пошкодженими і недійсними кадрами.

Рисунок 3.1 – Комутація з проміжним збереженням

В режимі наскрізної комутації комутатор може прийняти рішення про переадресацію, щойно визначить MAC-адресу призначення кадру в таблиці MAC-адрес, як показано на рисунку 3.2. Для прийняття рішення про пересилання комутатору не потрібно чекати решти частин кадру, що надходить через вхідний інтерфейс. Отже, наскрізна комутація має можливість виконувати швидку комутацію кадрів. Завдяки невеликій затримці наскрізна комутація краще підходить для ресурсномістких застосунків, що виконують високопродуктивні обчислення (HPC), для яких затримка між процесами повинна складати не більше 10 мікросекунд.

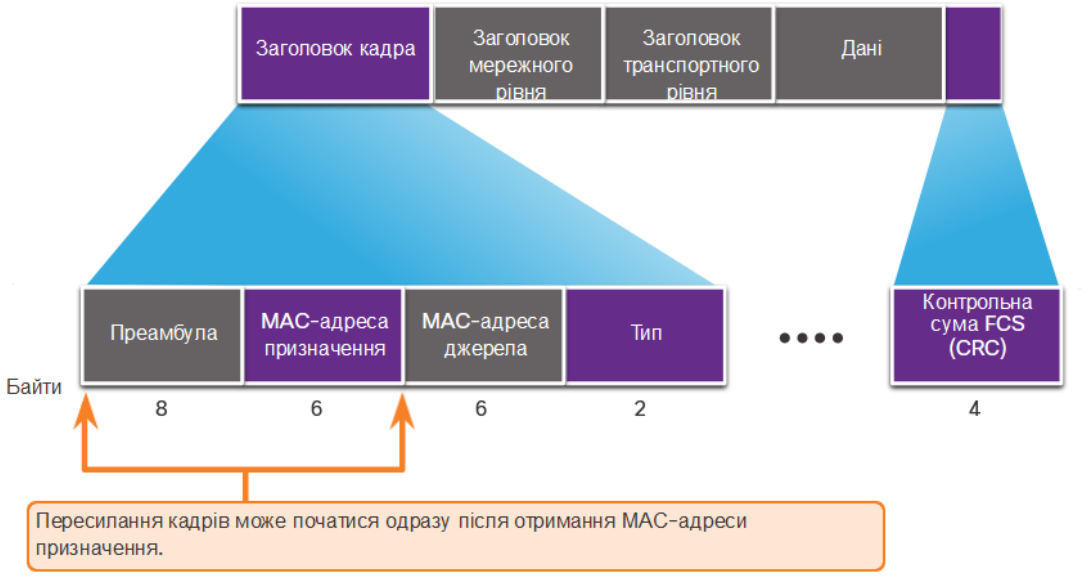


Рисунок 3.2 – Наскрізна комутація

3.1.3. Типи та побудова базового мережного устаткування

Комутаційний центр це пункт мережі, який забезпечує регенерацію сигналів і (можливо) розподіл інформації в мережі згідно з заданою адресою. КЦ також називають вузлом мережі. **Для апаратної реалізації вузлів використовують:**

– *Мережні карти.*

Устаткування, що зв'язує кінцевого користувача з мережею, їх називають також кінцевими вузлами або станціями (host) і реалізується у вигляді плати мережного інтерфейсу (Network Interface Card – NIC) або мережного адаптера (рисунок 3.3).

– *Повторювачі (repeater).*

Представляють собою мережне обладнання (рисунок 3.4), яке функціонує на першому (фізичному) рівні еталонної моделі OSI. Метою використання повторювача є регенерація та синхронізація мережних сигналів на битовом рівні, що дозволяє передавати їх по середовищі на більшу відстань.

– *Концентратори (hub).*

Один з видів мережного обладнання (рисунок 3.5), яке можна встановлювати на рівні доступу мережі Ethernet. На концентраторах є кілька інтерфейсів для підключення вузлів до мережі. Концентратори це просте обладнання, він не в змозі визначити, якому вузлу призначене конкретне повідомлення. Він просто бере електронні сигнали одного інтерфейсу і відтворює (або ретранслює) те саме повідомлення для всіх інших інтерфейсів.

Рисунок 3.3 – Мережний адаптер (NIC)

Рисунок 3.4 –Повторювач (Repeater)

– *Мости (bridge).*

Представляють собою обладнання другого рівня (рисунок 3.6), призначене для створення двох сегментів мережі. Міст збирає інформацію про те, на який його стороні (порту) знаходиться конкретний MAC-адреса, і приймає рішення щодо пересилання даних на підставі відповідного списку MAC-адрес. Мости здійснюють фільтрацію потоків даних на основі тільки MAC-адреса вузлів. З цієї причини вони можуть швидко пересилати дані будь-яких протоколів мережного рівня.

Рисунок 3.5– Концентратор

3.6 – Міст

– *Комутатори (switch).*

Комутатор з’єднує кілька вузлів з мережею. На відміну від концентратора, комутатор є пристроєм канального рівня (рисунок 3.7) і здійснює передачу повідомлення конкретному вузлу. Коли вузол відправляє повідомлення іншого вузла через комутатор, той приймає, декодує кадри і зчитує фізичний (MAC) адреса призначення повідомлення. Далі здійснює відправку на порт відповідний цій адресі.

– *Маршрутизатор (router).*

Являють собою обладнання об’єднаних мереж (рисунок 3.8), які пересилають пакети між мережами на основі адрес третього рівня. Маршрутизатор є високоінтелектуальним пристроєм, що дозволяє також реалізовувати багато додаткових функцій.

3.7 – Комутатори
Cisco серії Catalyst 6500

Рисунок 3.8 – Маршрутизатор
Cisco 1841

Наведене обладнання є основним, проте є ще величезний перелік спеціалізованого мережного обладнання, типу модеми, брандмауери (firewall), мовні шлюзи і т.д.

3.1.4. Структуризація мереж

У локальних мережах з невеликою кількістю комп’ютерів (10÷30) частіше усього використовують технології та структури які забезпечують

властивість однорідності, тобто всі комп'ютери в такій мережі мають однакові права у відношенні доступу до інших комп'ютерів. Така однорідність структури спрощує процедуру нарощування числа комп'ютерів, полегшує обслуговування й експлуатацію мережі.

Однак при побудові великих мереж однорідна структура зв'язків перетворюється з переваги в недолік. **У таких мережах використання типових структур породжує різноманітні обмеження, найважливішими з яких є:**

- обмеження на довжину зв'язку між вузлами;
- обмеження на кількість вузлів у мережі;
- обмеження на інтенсивність трафіка, що генерують вузли мережі.

Наприклад, технологія ***Ethernet*** на тонкому коаксіальному кабелі дозволяє використовувати кабель довжиною не більш 185 метрів, до якого можна підключити не більш 30 комп'ютерів. Однак якщо комп'ютери інтенсивно обмінюються інформацією, іноді приходиться знижувати число підключених до кабелю машин до 20, а то і до 10, щоб кожному комп'ютеру діставалася прийнятна частка загальної пропускної здатності мережі.

Для зняття цих обмежень використовуються особливі методи структуризації мережі і спеціальне структуроутворююче устаткування – повторювачі, концентратори, мости, комутатори, маршрутизатори. Такого роду устаткування також називають комунікаційним, маючи на увазі, що з його допомогою окремі сегменти мережі взаємодіють між собою.

Розрізняють:

1. Топологію фізичних зв'язків (фізичну структуру мережі). У цьому випадку конфігурація фізичних зв'язків визначається електричними з'єднаннями комп'ютерів, тобто ребрам графа відповідають відрізки кабелю, що зв'язують пари вузлів.

2. Топологію логічних зв'язків (логічну структуру мережі). Тут як логічні зв'язки виступають маршрути передачі даних між вузлами мережі, що утворяться шляхом відповідної настройки комунікаційного устаткування.

Фізична структуризація мережі

Під **фізичною топологією** розуміється конфігурація зв'язків, утворених окремими частинами кабелю.

Отже фізична структуризація реалізується шляхом вибору певної структури мережі. Вибір варіанту структури ЛМ визначається в основному оперативними умовами (умовами управління), відношенням між навантаженням і пропускною спроможністю каналів, характеристиками технічних комплексів передачі даних.

Шина

Фізична топологія шина, що іменується також лінійною шиною, складається з єдиного кабелю, до якого приєднані усі комп'ютери сегменту (рисунок 3.9).

Повідомлення посилаються по лінії усім підключеним станціям незалежно від того, хто є одержувачем. Кожен комп’ютер перевіряє кожен пакет в дроті, щоб визначити одержувача пакету. Якщо пакет призначений для іншої станції, то комп’ютер відкидає його. Якщо пакет призначений цьому комп’ютеру, то він отримає і обробить його.

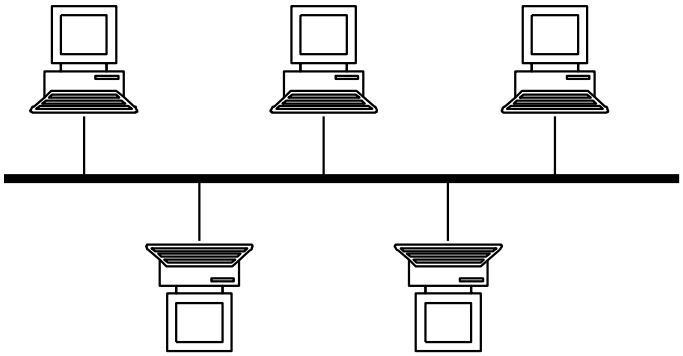


Рисунок 3.9 – Топологія "шина"

Головний кабель шини, відомий як магістраль, має на обох кінцях заглушки (термінатори) для запобігання віддзеркаленню сигналу.

Недоліки:

– важко ізолювати неполадки станції або іншого мережного компонента;

– неполадки в магістральному кабелі можуть привести до виходу з ладу усієї мережі.

Кільце

У фізичній топології "кільце" лінії передачі даних фактично утворюють логічне кільце, до якого підключені усі комп’ютери мережі (рисунок 3.10).

Доступ до носія в кільці здійснюється за допомогою маркерів (token), які пускаються по кругу від станції до станції, даючи їм можливість переслати пакет, якщо це треба. Комп’ютер може посилати дані тільки тоді, коли володіє маркером.

Оскільки кожен комп’ютер при цій топології є частиною кільця, він має можливість пересилати будь-які отримані ним пакети даних, адресовані іншій станції.

Недоліки:

– неполадки на одній станції можуть привести до відмови усієї мережі;

– при переконфігурації будь-якої частини мережі необхідно тимчасово відключати усю мережу.

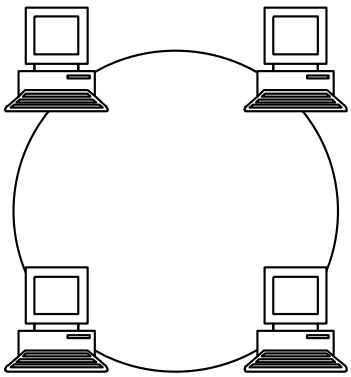


Рисунок 3.10 – Топологія "кільце"

Зірка

У топології Star (зірка) усі комп’ютери в мережі сполучені один з одним за допомогою центрального концентратора (рисунок 3.11).

Усі дані, які посилає станція, прямують прямо на концентратор, який пересилає пакет у напрямі одержувача.

У цій топології тільки один комп’ютер може посилати дані в конкретний момент часу. При одночасній спробі двох і більше комп’ютерів переслати дані, усі вони дістануть відмову і будуть вимушені чекати випадковий інтервал часу, щоб спробувати ще раз.

Ці мережі краще масштабуються, чим інші мережі. Неполадки на одній станції не виводять з ладу усю мережу. Наявність центрального концентратора полегшує додавання нового комп’ютера.

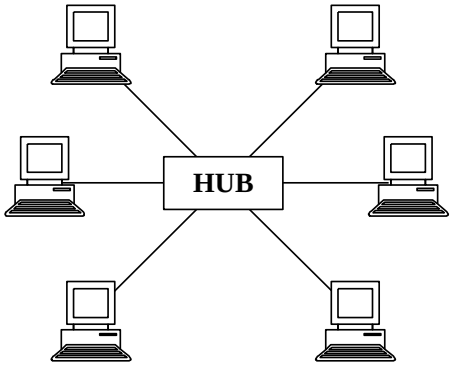


Рисунок 3.11 – Топологія "зірка"

Недоліки:

– вимагає більше кабелю, чим інші топології;
– вихід з ладу концентратора виведе з ладу увесь сегмент мережі.

Комірка

Топологія Mesh (комірка) сполучає усі комп’ютери попарно (рисунок 3.12). Мережі Mesh використовують значно більшу кількість кабелю, чим інші топології. Ці мережі значно важче встановлювати. Але ці мережі стійкі до збоїв (здатні працювати за наявності ушкоджень).

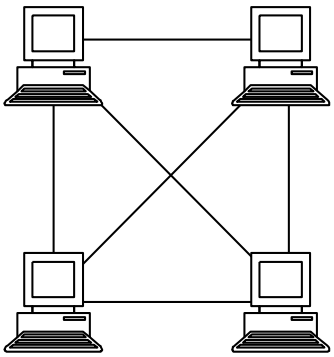


Рисунок 3.12 – Топологія "комірка"

Пристрої для фізичного з'єднання

1. Найпростіший з комунікаційних пристроїв – повторювач (***repeator***) – використовується для фізичного з'єднання різних сегментів кабелю локальної мережі з метою збільшення загальної довжини мережі. Повторювач передає сигнали, що приходять з одного сегмента мережі, в інші її сегменти (рисунок 3.13). Повторювач дозволяє перебороти обмеження на довжину ліній зв'язку за рахунок поліпшення якості переданого сигналу – відновлення його потужності й амплітуди, поліпшення і відновлення фронтів і т.п.

2. Повторювач, що має кілька портів і з'єднує кілька фізичних сегментів, часто називають концентратором (***concentrator***) чи хабом (***hub***). Ці назви (***hub*** – основа, центр діяльності) відбивають той факт, що в даному пристрої зосереджені всі зв'язки між сегментами мережі.

Використання концентраторів характерно практично для всіх базових технологій локальних мереж – ***Ethernet***, ***ArcNet***, ***Token Ring***, **FDDI**, ***Fast Ethernet***, ***Gigabit Ethernet***.

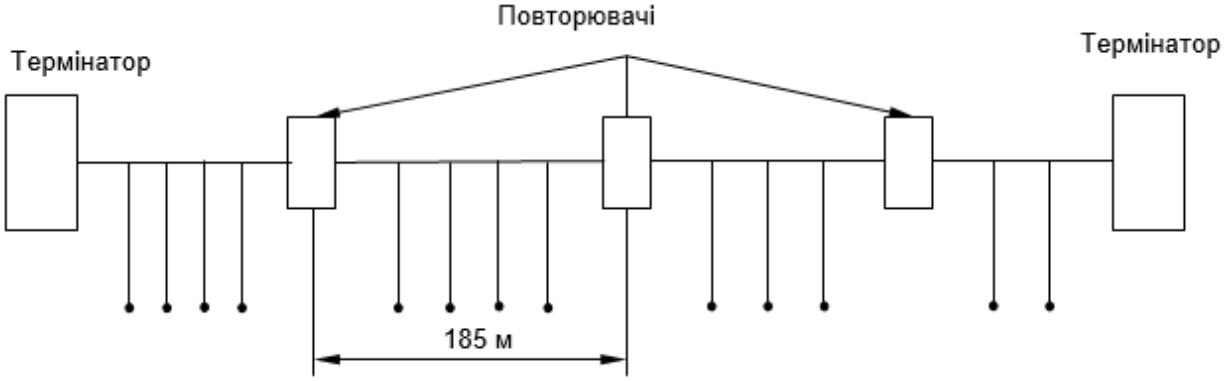


Рисунок 3.13 – Повторювач дозволяє збільшити довжину мережі

Потрібно підкреслити, що в роботі будь-яких концентраторів багато спільного – вони повторюють сигнали, що прийшли з одного з їхніх портів, на інших своїх портах. Різниця полягає в тому, на яких саме портах повторюються вхідні сигнали. Так, концентратор ***Ethernet*** повторює вхідні сигнали на усіх своїх портах, крім того, з якого сигнали надходять (рисунок 3.14).

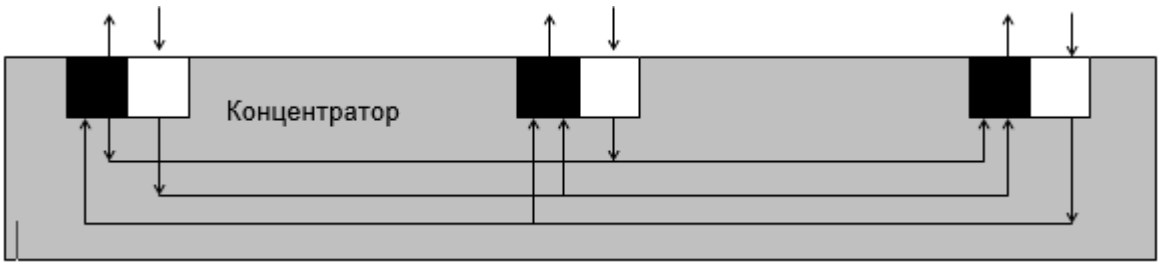


Рисунок 3.14 – Робота Концентратор

Фізична структуризація мережі корисна в багатьох відношеннях, однак у ряді випадків, що звичайно відносяться до мереж великого і середнього розміру, без логічної структуризації мережі обійтися неможливо. Найбільш важливою проблемою, не розв'язуваною шляхом фізичної структуризації, залишається проблема перерозподілу переданого трафіка між різними фізичними сегментами мережі.

Логічна структуризація мережі

Логічна структуризація мережі – це процес розбивки мережі на сегменти з локалізованим трафіком.

Для підвищення ефективності роботи мережі необхідно враховувати неоднорідність інформаційних потоків (внутрішній або зовнішній трафік наприклад).

Поширення трафіка, призначеного для комп'ютерів деякого сегмента мережі, тільки в межах цього сегмента, називається локалізацією трафіка.

Для логічної структуризації мережі використовуються комунікаційні пристрої, що можуть аналізувати певні атрибути інформації, адреси призначення, номери портів призначення, види протоколів і т.д.:

- мости;
- комутатори;
- маршрутизатори;
- шлюзи.

Міст (***bridge***) пристрій, що поділяє середовище передачі мережі на частини (які часто називають логічними сегментами), передаючи інформацію з одного сегмента в інший тільки в тому випадку, якщо така передача звісно необхідна, тобто якщо адреса комп'ютера призначення належить іншій підмережі. Тим самим міст ізолює трафік однієї підмережі від трафіка іншої, підвищуючи загальну продуктивність передачі даних у мережі. Локалізація трафіка не тільки заощаджує пропускну здатність, але і зменшує можливість несанкціонованого доступу до даних, тому що кадри не виходять за межі свого сегмента, і зловмиснику складніше перехопити їх.

На рисунку 3.15 показана мережа, що була отримана з мережі з центральним концентратором шляхом його заміни на міст. Мережі 1-го і 3-го відділів є окремими логічними сегментами, в середині яких пристрої з'єднані через концентратор. Тобто кожен логічний сегмент, побудований на базі концентратора, має найпростішу фізичну структуру, утворену відрізками кабелю, що зв'язують комп'ютери з інтерфейсами концентратора. Якщо

користувач комп'ютера А відправить дані користувачу комп'ютера В, що знаходиться в одному з ним сегменті, то ці дані будуть повторені тільки на тих мережних інтерфейсах, що відзначені на рисунку заштрихованими кружками.

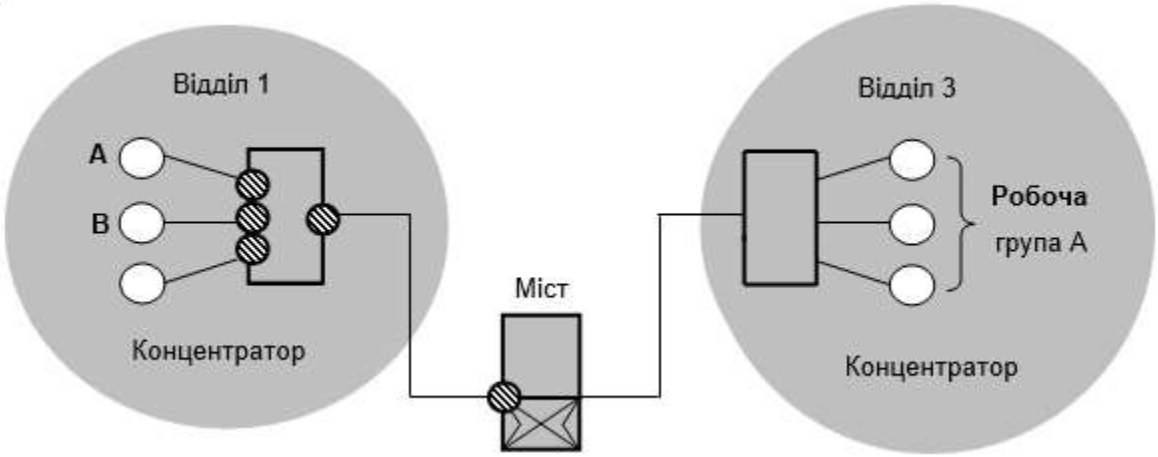


Рисунок 3.15 – Міст Ethernet

Мости використовують для локалізації трафіка апаратні (фізичні) адреси комп'ютерів. Це ускладнює розпізнавання приналежності того чи іншого комп'ютера до визначеного логічного сегмента – сама адреса не містить подібної інформації.

Тому міст досить спрощено представляє розподіл мережі на сегменти – він запам'ятовує, через який інтерфейс на нього надійшов кадр даних від кожного комп'ютера мережі, і надалі передає кадри, призначені для даного комп'ютера, на цей інтерфейс. Точної топології зв'язків між логічними сегментами міст не знає. Через це застосування мостів приводить до значних обмежень на конфігурацію зв'язків мережі – сегменти повинні бути з'єднані таким чином, щоб у мережі не утворювалися замкнуті контури.

Комутатор (***switch***) за принципом обробки кадрів від моста практично нічим не відрізняється. Його відмінності полягають в тому, що він має більш ніж два інтерфейси та є свого роду комунікаційним мультипроцесором. Кожен інтерфейс комутатора оснащений спеціалізованою мікросхемою, що обробляє кадри по алгоритму моста незалежно від мікросхем інших інтерфейсів. За рахунок цього загальна продуктивність комутатора звичайно набагато вище продуктивності традиційного моста, що має один процесорний блок. Можна сказати, що комутатори – це мости нового покоління, що обробляють кадри в рівнобіжному режимі.

В комутаторах з'являється також додаткова можливість структуризації на основі **віртуальних мереж VLAN**, тобто обмеження поширення трафіку на основі позначення кадрів інформації спеціальними заголовками – **тегами**. VLAN – це віртуальне відокремлення частини інтерфейсів комутатора, що забезпечує сегментацію та організаційну гнучкість у комутованій мережі. VLAN базуються на логічних зв'язках, а не на фізичних з'єднаннях.

Як показано на рисунку 3.16, VLAN у комутованій мережі дають змогу користувачам різних відділів (Faculty, Student і Guest) підключатися до однієї відокремленої мережі незалежно від використовуваного фізичного комутатора або розташування в кампусній локальній мережі.

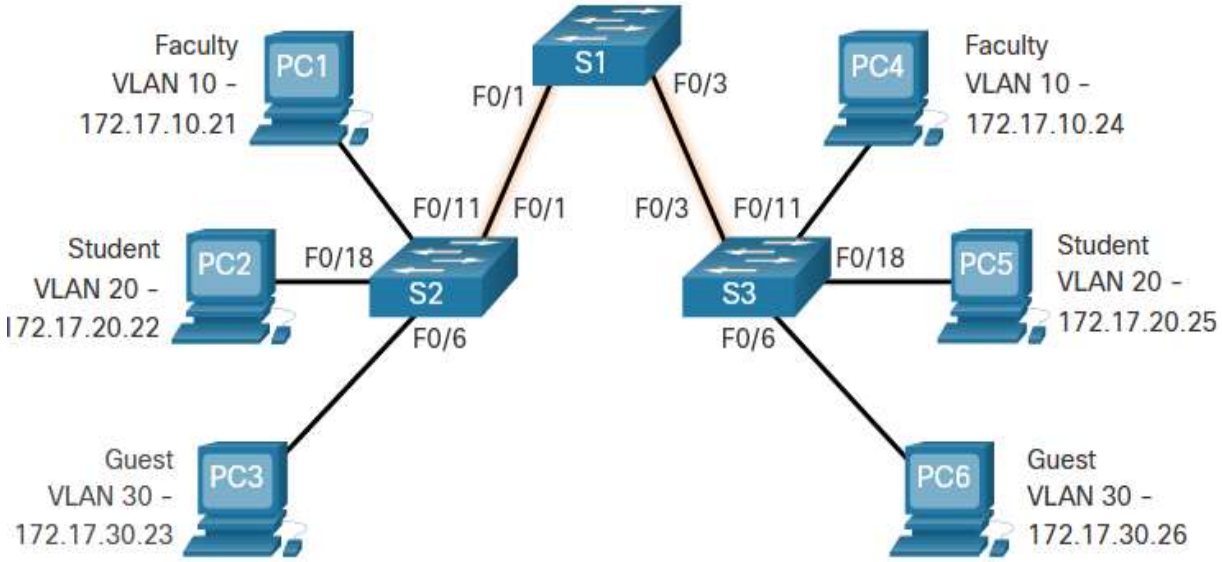


Рисунок 3.16 – Приклад використання VLAN

У таблиці 3.1 наведені переваги проектування мережі з VLAN.

Стандартний заголовок кадру Ethernet не містить інформації про VLAN, якій належить кадр. Тому при передаванні Ethernet-кадрів необхідно додати інформацію про VLAN, до яких належать ці кадри. Цей процес носить назву "тегування" і реалізовується за допомогою заголовка IEEE 802.1Q, описаного у стандарті IEEE 802.1Q. Заголовок 802.1Q містить 4-байтний тег (рисунок 3.17), який додається в оригінальний заголовок Ethernet-кадру, і саме в ньому вказується VLAN, якій належить кадр.

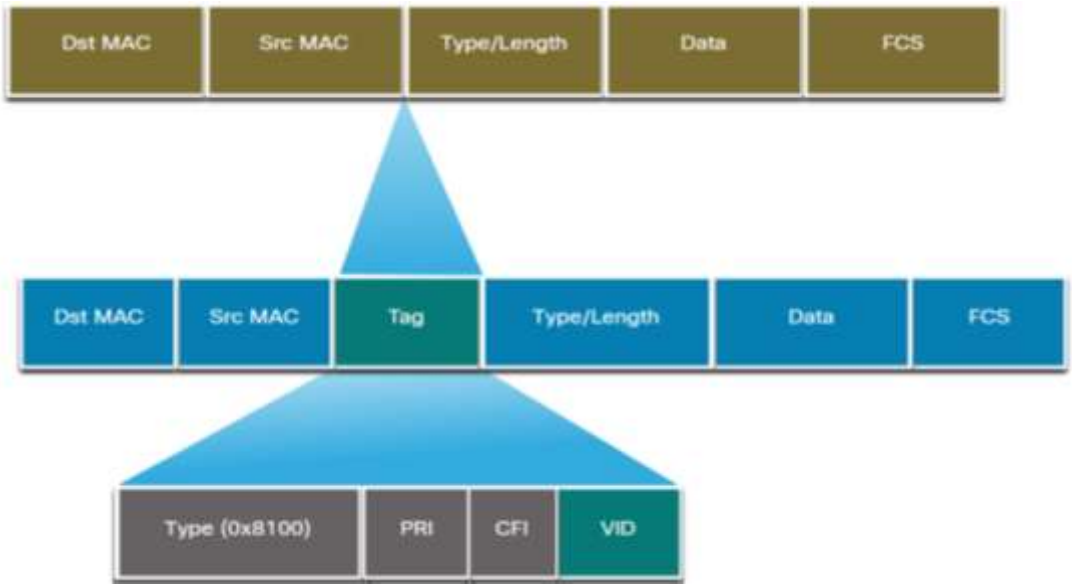


Рисунок 3.17 – Заголовок 802.1Q (VLAN)

Таблиця 3.1 – Переваги проектування мережі з VLAN

Переваги	Опис
Менший широкомовний домен	• Поділ мережі на VLAN зменшує кількість пристроїв у широкомовному домені. • У мережі, що наведена на рисунку, є шість комп'ютерів, але лише три широкомовні домени (Faculty, Student, and Guest).
Покращена безпека	• Спілкуватися один з одним можуть тільки користувачі однієї VLAN. • На рисунку показано, що мережний трафік підрозділу Faculty (VLAN 10) повністю відокремлений та захищений від користувачів інших VLAN.
Підвищення ефективності IT-інфраструктури	• VLAN спрощують управління мережею, тому що користувачі з однаковими мережними потребами можуть бути налаштовані в одній і тій же VLAN. • Для полегшення ідентифікації VLAN можуть мати назви. • На рисунку VLAN 10 має назву "Faculty", VLAN 20 – "Student", VLAN 30 – "Guest".
Зниження витрат	• VLAN зменшують потребу у високовартісній модернізацій мережі та дають змогу використовувати існуючу пропускну здатність і висхідні канали зв'язку більш ефективно, як наслідок витрати зменшуються.
Краща продуктивність	• Менші широкомовні домени скорочують об'єм непотрібного трафіку у мережі і покращують продуктивність мережі в цілому.
Простіше керування проектами та застосунками	• VLAN об'єднують користувачів та мережні пристрої для забезпечення виробничих вимог або вимог щодо розміщення. • Наявність окремих функцій дозволяє спростити керування проектом або роботу зі спеціалізованим застосунком; прикладом такого застосунку є факультетська платформа для електронного навчання.

Коли комутатор отримує кадр на інтерфейсу, що належить певній VLAN і налаштованому для функціонування в режимі доступу, комутатор додає тег VLAN в заголовок кадру, заново розраховує значення поля FCS і надсилає тегований кадр далі.

Як показано на рисунку 3.17, інформаційне поле керування тегами VLAN складається з полів:

- "Тип" (Type) – 2-байтне значення, яке називається ідентифікатором протоколу тега (TPID, Tag Protocol Identifier). Для технологій Ethernet – це шістнадцяткове значення 0x8100;
- "Пріоритет" (PRI, User Priority) – 3-бітне значення, яке підтримує реалізацію рівня чи служби (клас обслуговування);
- "Ідентифікатор канонічного формату" (CFI, Canonical Format Identifie) – 1-бітний ідентифікатор, який дозволяє передавати кадри технології Token Ring через канали мережі Ethernet;
- "Ідентифікатор VLAN"(VID, VLAN ID, VLAN Identifier) – 12-бітний ідентифікаційний номер VLAN, що може містити до 4096 номерів VLAN.

В залежності від налаштування та призначення VLAN можуть бути різного типу. Відомі VLAN п’яти наступних типів:

1. VLAN за замовчуванням

VLAN за замовчуванням (Default VLAN) на комутаторі Cisco – це VLAN 1. Слід пам’ятати про VLAN 1 такі важливі факти:

- За замовчуванням всі інтерфейси комутатора належать до VLAN 1.
- За замовчуванням VLAN з нетегованим трафіком (Native VLAN) – це VLAN 1.
- За замовчуванням управлінська VLAN (Management VLAN) – це VLAN 1.
- Не можна перейменувати або видалити VLAN 1.

2. VLAN даних

VLAN даних (Data VLAN) – це VLAN, налаштовані для відокремлення трафіку, що створюється користувачами. Такі VLAN також називають VLAN користувачів, бо саме вони розділяють мережу на групи користувачів або групи пристроїв. Залежно від організаційних вимог сучасна мережа матиме багато VLAN даних. Голосовий трафік і трафік управління мережею не повинні передаватися у VLAN даних.

3. Управлінська VLAN

Управлінська VLAN – це VLAN даних, спеціально налаштована для передавання трафіку управління мережею, зокрема, трафіку протоколів SSH, Telnet, HTTPS, HHTP і SNMP.

4. Голосова VLAN

Для підтримки технології VoIP (Voice over IP) потрібна окрема VLAN, це пов’язане з особливими вимогами до VoIP трафіку з точки зору гарантованої пропускної здатності, уникнення перевантажених ділянок мережі, пріоритетного обслуговування у проміжних вузлах та мінімізації затримки.

Використання VLAN було б не можливим без *транкових (магістральних) каналів VLAN*. Транкові канали VLAN змогу пристроям, які підключені до різних комутаторів, але належать одній VLAN, взаємодіяти без передачі трафіку через маршрутизатор. ***Транковий канал*** – це двоточковий канал зв’язку між мережними пристроями, який дає змогу передавати трафік більше ніж однієї VLAN. Cisco підтримує стандарт IEEE 802.1Q для узгодження магістральних каналів на інтерфейсах технологій Fast Ethernet, Gigabit Ethernet та 10-Gigabit Ethernet. Транковий канал VLAN не належить до певної VLAN – він є каналом передавання трафіку декількох VLAN між комутаторами і маршрутизаторами. Транковий канал також може використовуватися між мережним пристроєм і сервером або іншим пристроєм, який оснащений мережною платою з підтримкою 802.1Q.

На рисунку 3.16 кольором виділені зв’язки між комутаторами S1 та S2, S1 та S3, які встановлені в режим транкового каналу і налаштовані на передачу трафіку, що надходить у мережу від VLAN 10, 20, 30 та 99 (Native VLAN).

5. Native VLAN

Native VLAN – це один з VLAN комутатора, на який покладена функція для обробки нетегованого трафіку. Такий трафік генерується самим комутатором або може надходити з застарілих пристроїв. Трафік згенерований у Native VLAN розміщується у транковому каналі 802.1Q без додавання тегу. Нетегований трафік на виході транкового каналу розподіляється у Native VLAN.

Обмеження, зв'язані з застосуванням мостів і комутаторів – по топології зв'язків, а також ряд інших, – привели до того, що в ряді комунікаційних пристроїв з'явився ще один тип устаткування – **маршрутизатор** (***router***). Маршрутизатори більш надійно і більш ефективно ніж мости, ізолюють трафік окремих частин мережі один від іншого. Маршрутизатори утворюють логічні сегменти за допомогою явної адресації, оскільки використовують не апаратні, а складені числові адреси (мережені). У цих адресах мається поле номера мережі, так що всі комп'ютери, у яких значення цього поля однакове, належать одному сегменту, який називають в даному випадку підмережею (***subnet***).

Крім локалізації трафіка, маршрутизатори виконують ще багато інших корисних функцій. Так, маршрутизатори можуть працювати в мережі з замкнутими контурами, при цьому вони здійснюють вибір найбільш раціонального маршруту з декількох можливих. Так мережа з рисунку 3.15 може бути доповнена тим, що між підмережами відділів 1 і 2 прокладено додатковий зв'язок, який може використовуватися для підвищення як продуктивності мережі, так і її надійності (рисунок 3.18).

Іншою дуже важливою функцією маршрутизаторів є їхня здатність зв'язувати в єдину мережу підмережі, побудовані з використанням різних мережних технологій, наприклад *Ethernet* і X.25.

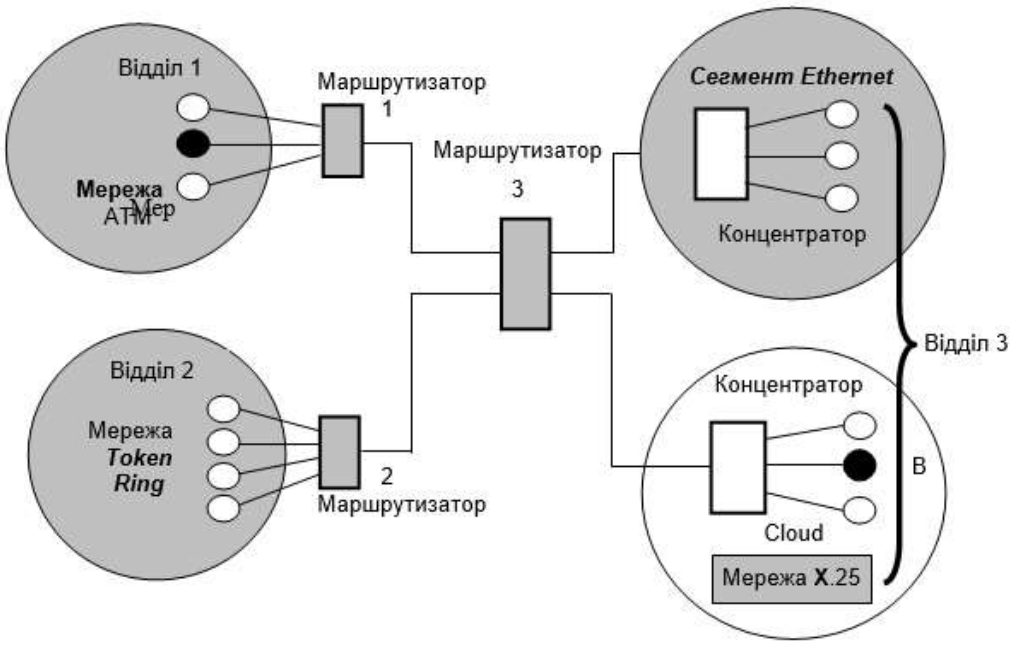


Рисунок 3.18 – Логічна структуризація мережі за допомогою маршрутизаторів

Крім перерахованих пристроїв, окремі частини мережі може з'єднувати **шлюз** (***gateway***). Звичайно основною причиною використання шлюзу в мережі є необхідність об'єднати мережі з різними типами системного і прикладного програмного забезпечення, а не бажання локалізувати трафік. Проте, шлюз забезпечує і локалізацію трафіка як певний побічний ефект.

Великі мережі практично ніколи не будуються без логічної структуризації. Для окремих сегментів і підмереж характерні типові однорідні топології базових технологій, і для їхнього об'єднання завжди використовується устаткування, що забезпечує локалізацію трафіка: мости, комутатори, маршрутизатори і шлюзи.

3.2. Адресування в телекомунікаційних та інформаційних мережах

3.2.1. Фізичні адреси

Для ідентифікації абонентів і знаходження місця їх розташування в мережі кожному з них привласнюється ознака – адреса.

Під адресою розуміється умовний номер, знання якого є достатнім для доставки повідомлення необхідному абонентові.

Сукупність правил присвоєння адрес абонентів, з обліком місць їх розташування й структури мережі називається *способом адресування*.

Існуючий стек протоколів пакетних мереж використовує три типи адрес:

- локальні (називаємі апаратними фізичними адресами);
- мережні (IP-адреси);
- символьні (доменні імена).

Фізична локальна адреса – це адреса, що використовується для доставки даних в локальних межах (підмережах), які є елементами складної мережі. Фізична локальна адреса – це **MAC-адреса** (***Media Access Control***), яка призначається мережним адаптерам і мережним інтерфейсам маршрутизаторів, інтерфейсам ПК і усім інтерфейсам елементів мережі. MAC-адреса назначається виробником обладнання і є унікальною, так як управляється централізовано. Для усіх відомих технологій ЛОМ MAC-адреса (рисунок 3.19) має формат 48 біт (6 октетів), наприклад: 11-A0-17-3D-BC-01.

MAC-адресу можна розділити на дві частини (рисунок 3.19). У першій частині вказується *унікальний ідентифікатор виробника встаткування* (Organizationally Unique Identifier, OUI). Цей унікальний ідентифікатор привласнюється виробникові інститутом IEEE.

Останні 24 біта MAC-адреси призначаються безпосередньо виробником устаткування. Перший біт MAC-адреси (I/G) указує, чи є адреса індивідуальною або груповою:

- 0 (індивідуальна) – адреса, асоційована з певним мережним пристроєм;
- 1 (групова) – адреса, асоційована з кількома або всіма вузлами даної мережі.

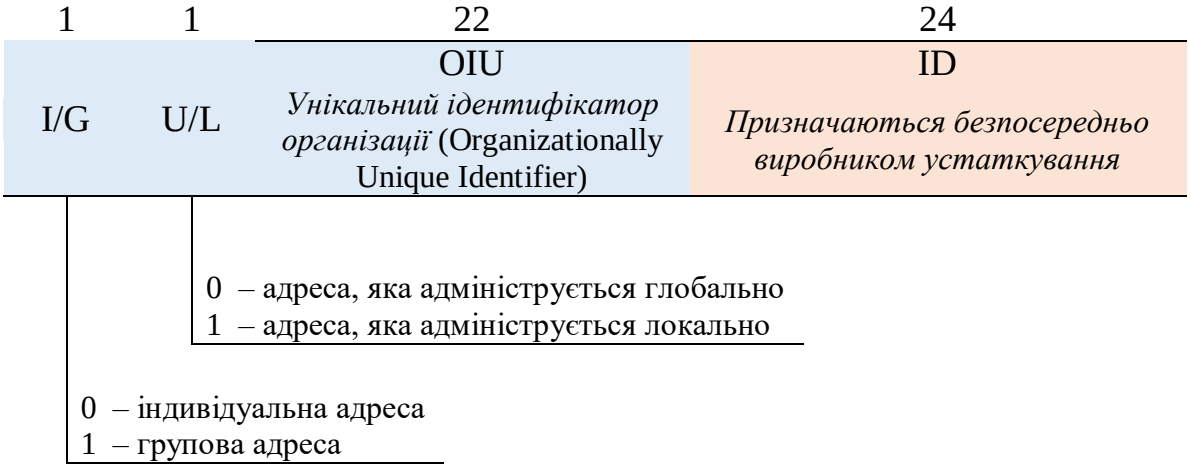


Рисунок 3.19 – Формат MAC-адреси

Існує два види групових адрес:

- *багатоадресна* або *групова* (*multicast*) – адреса, асоційована із групою вузлів мережі;
- *широкомовна* (*broadcast*) – адреса, асоційована з усіма вузлами мережі. Її значення – (0x11)F-FF-FF-FF-FF-FF.

Другий біт MAC-адреси (U/L) указує, чи є MAC-адреса глобально або локально адмініструєма:

- 0 (глобально адмініструєма MAC-адреса пристрою) – вона глобально унікальна (адмініструється IEEE) і звичайно "зашита" в апаратуру;
- 1 (локально адмініструєма MAC-адреса) – вона вибирається довільно й може не містити інформації про виробника даного встаткування (OUI). Деякі виробники мережних адаптерів підтримують можливість змінювати MAC-адреси пристрою.

3.2.2. Мережні адреси (IPv4)

IP-адреса або **адреса третього рівня** – це логічна адреса, яка не прив'язується до конкретної апаратури (мережній карті, інтерфейсу і т.д.) і призначається адміністратором мережі:

- **протокол IP версії 4 (IPv4) – використовує 32-бітні адреси;**

Класова адресація IPv4

Споконвічно розмір IPv 4-адреси був обраний довжиною в 32 біта (при цьому можна адресувати $2^{32} \approx 4{,}3$ млрд. пристроїв).

Хронологічно першим методом поділу IP-адрес є так звана класова модель IP-адресації, яка частково розв'язала проблему нераціонального використання адресного простору. Згідно із цією моделлю, увесь простір IP-адрес ділиться на 5 класів залежно від значення перших чотирьох біт IPv4-адреси. Класам привласнені імена від A до E (таблиця 3.2).

Перші 3 класи A, B и C використовуються для індивідуальної (unicast) адресації мереж і вузлів, клас D – для багатоадресного або групового (multicast) розсилання, клас E зарезервований для експериментів. Класи A, B и C мають різну довжину мережної частини адреси.

Для мереж класу A (рисунок 3.20) під ідентифікатор мережі приділяється 1 байт (перший октет), 3 байти (3 октети), що залишилися використовуються для ідентифікатора вузла, причому старший (лівий) біт ідентифікатора мережі завжди рівний 0.

Таблиця 3.2 – Класи IP-адрес

Клас	**Перші біти**	**Найменший номер мережі**	**Найбільший номер мережі**	**Максимальне число вузлів у мережі**
A	0	1.0.0.0	126.0.0.0	2^{24} (поле 3 байти)
B	10	128.0. 0.0	191. 255.0.0	2^{16} (поле 2 байти)
C	110	192.0. 0.0	223. 255.255.0	2^{8} (поле 1 байт)
D	1110	224.0. 0.0	239. 255.255.255	Групові адреси
E	11110	240.0. 0.0	247. 255.255.255	Зарезервований

Оскільки перший біт ідентифікатора мережі завжди дорівнює нулю, те 7 біт, що залишилися дозволяють адресувати 128 (2^7) різних мереж. Однак через те, що адреси 0.0.0.0 і 127.0.0.0 є спеціальними IPv4-адресами, кількість доступних мереж класу A рівно 126 (2^7-2). У кожній мережі класу A можна адресувати до 16 777 214 (2^{24}-2) вузлів. Дві адреси віднімаються внаслідок того, що вони використовуються в спеціальних цілях і не можуть бути призначені пристрою (перший – адреса мережі, останній – широкомовна адреса).

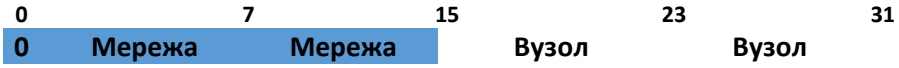


Рисунок 3.20 – Формат IPv 4-адреси класу A

Мережі класу B (рисунок 3.21) визначаються значеннями 10 у двох старших бітах адреси. Перші 2 байта в адресі використовуються для ідентифікатора мережі, 2 байта, що залишилися – для ідентифікатора вузла. У результаті кількість доступних мереж класу B становить 16 384 (2^{14}) з кількістю вузлів у кожній мережі рівним 65 534 (2^{16}-2).

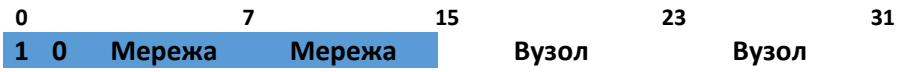


Рисунок 3.21 Формат IPv 4-адреси класу B

Для мереж класу 3 (рисунок 3.22) під ідентифікатор мережі приділяється 3 байта в той час як під ідентифікатор вузла тільки 1 байт. Три

старші біти першого октету завжди рівні 110, дозволяючи визначити, що адреса ставиться саме до класу С. Таким чином, одержуємо 2 097 152 (2^{21}) мереж, у кожній з яких перебуває 254 (2^8-2) вузла.

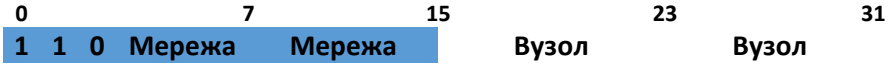


Рисунок 3.22 – Формат IPv 4-адреси класу З

Мережі класу D (рисунок 3.23) визначаються значеннями 1110 у перших чотирьох бітах адреси, інші біти використовуються для адресації багатоадресної групи. Адресний простір класу D зарезервоване для групового розсилання й використовується для адресації групи вузлів. Ідентифікаторів мереж і вузлів в IPv4-адресі класу D не виділяють.

Рисунок 3.23 – Формат IPv4-адреси класу D

Мережі класу E (рисунок 3.24) є експериментальними й у цей час не використовуються. Адреси в цьому класі визначаються значеннями 1111 у перших чотирьох бітах.

Рисунок 3.24 – Формат IPv 4-адреси класу E

Часткові й публічні адреси IPv4

У мережі Інтернет ідентифікація пристроїв здійснюється унікальними IPv4-адресами, які не повинні повторюватися в глобальній мережі. Такі IPv4-адреси називаються публічними адресами. Однак число публічних адрес обмежене, тому в кожному із класів IP-мереж визначений так званий частковий простір IP-адрес. Часткові IPv4-адреси призначені для використання в локальних комп'ютерних мережах і не маршрутизуються в Інтернет. Для локальних мереж, не підключених до мережі Інтернет, можна використовувати будь-які можливі адреси, унікальні в межах даної мережі.

Публічні адреси перебувають у межах від 1.0.0.1 до 223.255.255.254 за винятком часткових адрес IPv4.

Адресний простір часткових IPv4-адрес складається з 3 блоків:

- 10.0.0.0 … 10.255.255.255 (клас A);
- 172.16.0.0 … 172.31.255.255 (клас B);
- 192.168.0.0 … 192.168.255.255 (клас C).

Крім цього визначені IPv4-адреси (таблиця 3.3), які мають спеціальне призначення (спеціальні адреси).

Застосування IP-адресування на основі класового розподілу обмежує можливості раціонального використання всього переліку (пула) адрес в кожній мережі, тому в подальшому стали використовувати два додаткових варіанти IPv4: на основі підмереж та основі безкласового адресування.

3.2.3. Мережні адреси (IPv6)

– **Протокол IP версії 6 (IPv6) – використовує 128-бітні адреси**

Протокол IPv6 – це нова версія протоколу IP, яка розроблена в якості спадкоємця IPv4 і покликана розв'язати проблему вичерпання адресного простору. На відміну від адреси IPv4, яка має довжину 32 біта, розмір адреси IPv6 становить 128 біт, що дозволяє адресувати приблизно $3{,}4 \times 10^{38}$ інтерфейсів пристроїв. Адреса IPv6 відображається як вісім груп по чотири шістнадцяткові цифри, розділені двокрапкою Наприклад (рисунок 3.25), 2001:0DB8:AC10:FE01:0018:8BFF:FED8:E3E0.

Таблиця 3.3 – Спеціальні IP-адреси

Ідентифікатор мережі (ІМ)	**Ідентифікатор вузла (ІВ)**	**Опис**
Усі «0»	Усі «0»	0.0.0.0 – не відома IPv4-адреса. Використовується, наприклад, коли пристрій намагається одержати IPv4-адреса за допомогою протоколу DHCP
Усі «0»	ІВ	Вузол призначення належить тій же мережі, що й вузол-відправник, наприклад, 0.0.0.25
ІМ	Усі «0»	Адреса мережі, наприклад, 175.11.0.0
ІМ	Усі «1»	Обмежена широкомовна адреса (у межах даної IP-мережі), наприклад, 192.168.100.255
Усі «1»	Усі «1»	255.255.255.255 – «глобальна» широкомовна адреса
169.254.x.y	ІВ	Адреси, що автоматично призначаються, за відсутності сервера DHCP
127.0.0.1		Адреса інтерфейсу зворотної петлі (loopback), призначений для тестування встаткування без реального відправлення пакета

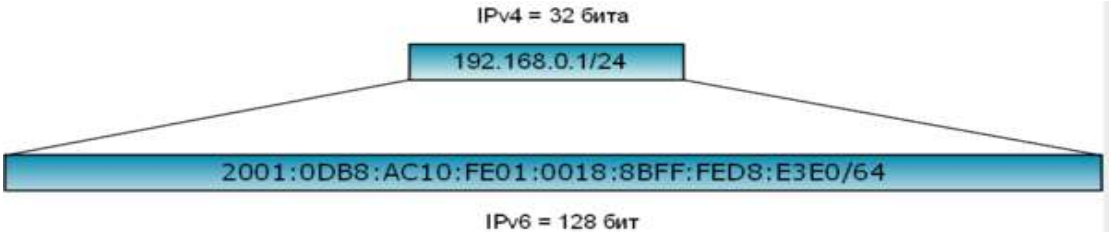


Рисунок 3.25 Адреси IPv4 і IPv6

Існує кілька способів, які дозволяють скоротити запис IPv6-адреси:

- нулі на початку групи можна замінити одним;
- одна або кілька послідовних груп, що складаються з нулів, можуть бути замінені позначкою "**::**", але тільки один раз;
- кінцеві нулі в групі повинні бути присутнім.

Для наведеної нижче адреси цифри, виділені жирним шрифтом, представляють позиції, у яких адреса може бути скорочена:

2001:1000:**0000**:**0000**:**0000**:ABCD:**0000**:**0001**

Варіанти можливих скорочень:

- 2001:1000::ABCD:0:0001;
- 2001:1000::ABCD:0:1.

IPv6-адреса складається із двох логічних частин – *префікса* (Prefix) і *ідентифікатора інтерфейсу* (Interface ID) (рисунок 3.26).

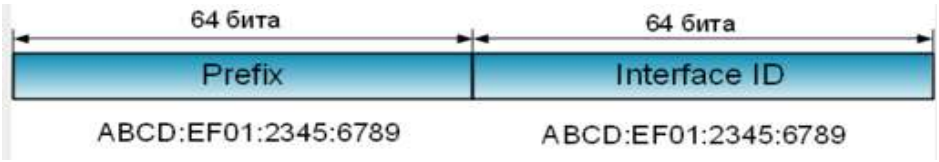


Рисунок 3.26 – Структура IPv6-адреси

***Префікс* (Prefix)** – перші 64 біти адреси, частина адреси, відведена під ідентифікатор мережі/підмережі (аналог ідентифікатора мережі в IPv4). Префікс адреси IPv6 записується у вигляді *адреса IPv6/довжина префікса*. Якщо довжина префіксу має значення 64, значить розбивка на підмережі не передбачена, якщо менше наприклад 48, то 48 біт відведені під номер мережі, а інша частина префіксу (64-48=16 біт) для номера підмережі:

Розглянемо для прикладу IPv6-адресу: 2001:0f68:0000:0000:0000:0000:1986:69af/48. Оскільки префікс (/48) указує на перші 48 біт, то 2001:0f68:0000 є номером мережі (Global Routing Prefix), а наступне поле, 0000, указує на ідентифікатор під мережі (Subnet ID).

***Ідентифікатор інтерфейсу* (Interface ID)** – останні 64 біта IPv6-адреси використовуються для ідентифікації інтерфейсу в сегменті мережі (аналог ідентифікатора вузла в IPv4). Він повинен бути унікальним усередині мережі/підмережі.

Адресний простір протоколу IPv6 розділений на три типи адрес:

- індивідуальні (unicast) адреси
- багатоадресні (multicast) адреси;
- альтернативні (anycast) адреси.

Індивідуальні адреси ідентифікують один інтерфейс пристрою. Пакети, відправлені на цю адресу, доставляються тільки на цей інтерфейс.

Типи Unicast адрес:

- *Глобальні*

Відповідають публічним IPv4 адресам. Можуть перебувати в будь-якому не зайнятому діапазоні. У цей час регіональні Інтернет-регістратори

розподіляють блок адрес 2000::/3 (з 2000:: по 3FFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF).

– *Link-Local*

Адреси мережі, які призначені тільки для комунікацій в межах одного сегмента місцевої мережі або магістральної лінії. Вони дозволяють звертатися до хостів, не використовуючи загальний префікс адреси. Маршрутизатори не відправлятимуть пакети з адресами link-local.

Адреси link-local часто використовуються для автоматичного конфігурування мережної адреси, у випадках, коли зовнішні джерела інформації про адресу мережі недоступні.

– *Unique-Local*

RFC 4193, відповідають частковим IP-адресам, якими у версії IPv4 були 10.0.0.0/8, 172.16.0.0/12 і 192.168.0.0/16. Починаються із цифр FC00 і FD00.

– *Групові адреси* IPv6, подібно однойменним адресам IPv4, визначають групу інтерфейсів. Пакети, що посилають на цю адресу, доставляються всім інтерфейсам – учасникам групи розсилання.

– *Альтернативні адреси* дозволяють адресувати групу інтерфейсів (звичайно приналежних різним вузлам). Однак на відміну від багатоадресних адрес, пакети, передані на альтернативну адресу, доставляються на один з інтерфейсів (звичайно “найближчий”, згідно з метрикою маршрутизації), обумовлених цією адресою.

– *Широкомовні адреси (Broadcast)*, які використовуються в IPv4, в IPv6 відсутні, що сприяє зменшенню мережного трафіка й зниженню навантаження на більшість систем. Широкомовні адреси замінені багатоадресними.

Серед IPv6-адрес також передбачені зарезервовані адреси (таблиця 3.4), які мають спеціальне призначення (спеціальні адреси).

Таблиця 3.4 – Зарезервовані адреси IPv6

IPv6 адреса	**Довжина префіксу (бітів)**	**Опис**	**Примітки**
::	128	Невизначена адреса	див. 0.0.0.0 в IPv4
::1	128	loopback адреса	див. 127.0.0.1 в IPv4
::ffff: xx.xx.xx.xx	96	Адреса IPv4, що відображена на IPv6	Нижні 32 біти – це адреса IPv4. Для хостів, що не підтримують IPv6.
2001:db8::	32	Документування	Зарезервовано для прикладів в документації в rfc3849
fe80:: – febf::	10	link-local	Аналог 169.254.0.0/16 в IPv4
fec0:: — feff::	10	site-local	Відмічений як застарілий в

			rfc3879
fc00::	7	Unique Local Unicast	Аналог 169.254.0.0/16 в IPv4
ffxx::	8	multicast	Мультімовлення для всіх маршрутизаторів ff02 :: 2 Мультімовлення для всіх вузлів ff02 :: 1

3.2.4. Символьні адреси

Символьні адреси, які в *Internet* називають доменними іменами застосовують для зручності роботи користувача у клієнтських програмах перегляду web-сторінок. Символьні адреси зазвичай несуть якесь смислове навантаження, їх набагато легше запам'ятовувати і вони формуються за ієрархічною ознакою. Складові повної символьної адреси в мережі розділяються крапкою і перераховуються в наступному порядку:

- спочатку ім’я кінцевого вузла, наприклад ***home***;
- потім ім’я групи вузлів, наприклад ***managers***;
- потім ім’я більшої групи, наприклад ***company***;
- і так до самого вищого рівня, наприклад ***ua***.

Символьні адреси зазвичай несуть якесь смислове навантаження і їх набагато легше запам'ятовувати, але реальна взаємодія вузлів все одно відбувається за IP-адресами. Тобто кожній символьній адресі співставляється певна IP-адреса. Проте між символьною адресою (доменним іменем) і IP-адресою вузла нема ніякої алгоритмічної відповідності, тому необхідні додаткові таблиці або служби, щоб вузол однозначно визначався, як по доменному імені, так і по IP-адресі.

В мережах на основі стеку TCP/IP використовується спеціальна служба ***Domain Name System*** (**DNS**), яка установлює цю відповідність на основі створюємих адміністраторами мережі *таблиць відповідності*. Тому доменні імена також називають DNS-імена.

Система DNS є ієрархічної й розподіленою. Не існує єдиної бази даних, що зберігає інформацію про всі імена та відповідні їм IP-адреси і інші записи. DNS – це мільйони баз даних, кожна з яких містить інформацію про конкретний домен. Ієрархію DNS можна побачити в доменному імені, наприклад, в імені веб-сайту. Візьмемо, наприклад, сайт – **www.cip.gov.ua**. Це ім’я складається із трьох частин, розділених крапками. Точніше чотирьох, оскільки, формально говорячи, повне доменне ім’я завжди закінчується крапкою, що позначає так званий кореневий домен, або кореневу зону DNS. Отже:

Коренева зона	Містить інформацію про всі піддомени: net, com, org, ru, su, і т.д. Точніше, інформацію про сервери, що обслуговують ці домени.
ua	Домен **ua**, що містить інформацію про всі піддомени, зареєстровані у ньому, наприклад, **gov**. Знову ж, цей домен містить адреси серверів, у яких можна одержати додаткову інформацію про вміст піддоменів.
gov	Домен **gov**, що містить інформацію про всі піддомени наступного, зареєстровані у ньому, зокрема **cip**. Знову ж, цей домен містить адреси серверів, у яких можна одержати додаткову інформацію про вміст піддоменів.
cip	Домен **cip**, що містить інформацію про всі служби або файли, а також імена серверів, зареєстрованих безпосередньо в цьому домені, зокрема **www.cip.gov.ua**
www	Послуга веб-сервера і відповідна йому IP-адреса.

Таким чином, трансляція імені www.cip.gov.ua у відповідну йому IP-адресу буде відбуватися в кілька етапів (рисунок 3.27). Спочатку будуть запитані сервери, що обслуговують кореневу зону. Ці сервери нічого не знають про існування доменів gov чи cip і тим більш адреси www.cip.gov.ua. Але вони повідомлять, як можна зв'язатися із серверами, що обслуговують домен наступного рівня ua (операції 2 та 3). Від них можна довідатися адреси серверів домену gov (операції 4 та 5). Від наступних – домену cip, які, у свою чергу, дадуть відповідь на запит про IP-адресу сервера www.cip.gov.ua.

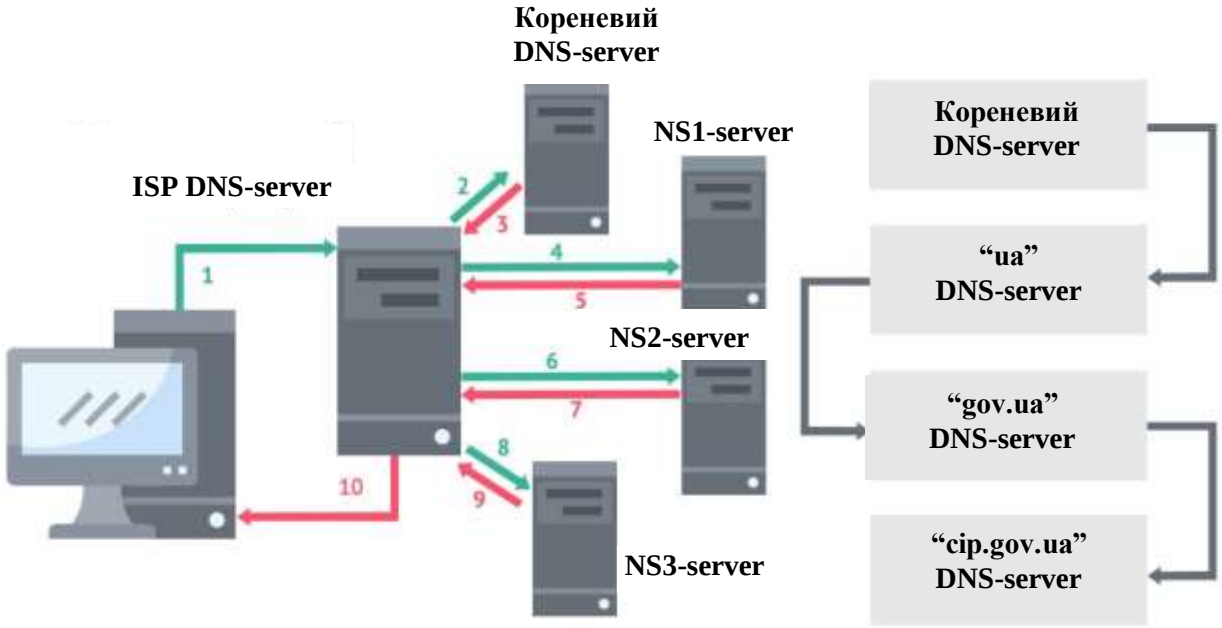


Рисунок 3.27 – Процес трансляції імен в DNS

Така архітектура DNS дозволяє розподілити навантаження й відповідальність за роботу системи між адміністраторами окремих доменів. До їхніх завдань входить забезпечення нормальної продуктивності при відповіді на запити до певної зони, підтримка унікальності імен у рамках

зони, а також повідомлення адміністраторові батьківської зони про зміни в складі серверів, що обслуговують зону.

3.3. Засоби ефективного використання пулів ip-адрес

3.3.1. Поняття маски IP-адреси

З появою трьохрівневої ієрархії IPv4-адрес потрібні були додаткові методи, які дозволяли б визначити, яка частина адреси вказує на ідентифікатор підмережі, а яка – на ідентифікатор вузла. Було запропоновано використовувати бітову маску (bit mask), яка відокремлювала б частину адресного простору ідентифікаторів вузлів від адресного простору ідентифікаторів підмережі. Така бітова маска називається ***маскою підмережі*** (subnet mask).

Маска підмережі (рисунок 3.28) – це 32-бітне число, двійковий запис якого містить одиниці в тих розрядах, які повинні визначатися як ідентифікатор мережі. Оскільки ідентифікатор мережі є цільною частиною IPv4-адреси, послідовність одиниць у масці підмережі повинна бути також безперервної.

Рисунок 3.28 – Формування маски підмережі

Щоб одержати адресу мережі, знаючи IPv4-адресу й маску підмережі, необхідно застосувати до них операцію *логічне "І"* (рисунок 3.29). Інакше кажучи, у тих позиціях IPv4-адреси, у яких в масці підмережі є двійкові 1, перебуває ідентифікатор мережі, а де двійкові 0 – ідентифікатор вузла.

Для мереж класу A, B и C визначені фіксовані маски підмережі, які жорстко визначають кількість можливих IPv4-адрес. Технологія поділу мережі дає можливість створювати більше число мереж з меншою кількістю вузлів у них, що дозволяє ефективно використовувати адресний простір.

Для обчислення кількості підмереж використовується формула 2^s, де s – кількість біт, зайнятих під ідентифікатор мережі із частини, відведеної під ідентифікатор вузла. Кількість вузлів у кожної підмережі обчислюється по формулі $2^n–2$, де n – кількість біт, що залишилися в частини, що ідентифікує вузол, а дві адреси – адреса підмережі й широкомовна адреса – у кожної отриманої підмережі зарезервовані.

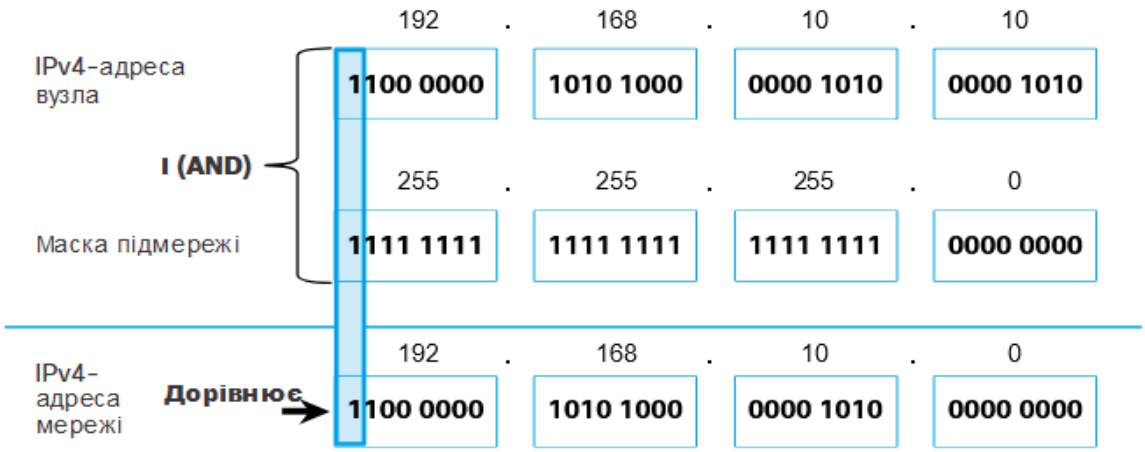


Рисунок 3.29 – Одержання адреси мережі з IP-адреси й маски підмережі

3.3.2. Адресування на основі підмереж

Для більш ефективного використання адресного простору були внесені зміни в існуючу класову систему адресації. В RFC 950 була описана процедура розбивки мереж на підмережі, і в структуру IPv4-адреси був доданий ще один рівень ієрархії – *підмереж* (subnetwork). Поява ще одного рівня ієрархії (рисунок 3.30) не змінило самої IPv4-адреси, вона залишилася 32-розрядною, а частина адреси, раніше відводилася під ідентифікатор вузла, була розділена на 2 частині – ідентифікатор підмережі й ідентифікатор вузла.

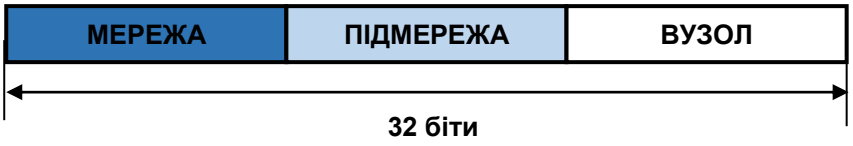


Рисунок 3.30 – Трьохрівнева ієрархія IP-адреси

Розбивка однієї великої мережі на більш дрібні (рисунок 3.31) дозволяє:

– раціонально використовувати адресний простір (тобто виділити для сегмента мережі блок адрес не цілком класу A, B або C, а тільки частину класової мережі);

– підвищити безпеку й керованість мережі (за рахунок зменшення розмірів сегментів і ізоляції трафіка сегментів один одного).

– Наприклад, організації необхідно розбити мережу 192.168.1.0 на 20 підмереж по 6 комп'ютерів у кожній. Для початку необхідно визначити, до якого класу відноситься адреса. 192.168.1.0 – це клас C, відповідно, стандартна маска підмережі для класу C дорівнює 255.255.255.0 і під ідентифікатор вузла відведений четвертий октет. Потім визначається кількість біт четвертого октету, потрібних для формування 20 підмереж. Оскільки знайти число, при якому ступінь 2 буде дорівнювати 20 неможливо,

вибираємо найближче більше число $2^5 = 32$. Таким чином, 5 перших біт 4-го октету будуть використані для ідентифікації підмережі, а 3 біта, що залишилися – для ідентифікації вузлів у них (рисунок 3.32).

–

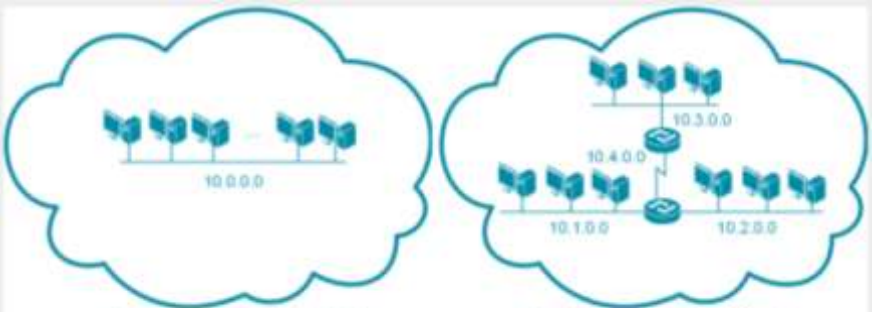


Рисунок 3.31 – Розбивка мережі на підмережі

Щоб уникнути проблем з адресацією й маршрутизацією всі мережні пристрої TCP/IP в одному сегменті мережі повинні використовувати ту саму маску підмережі.

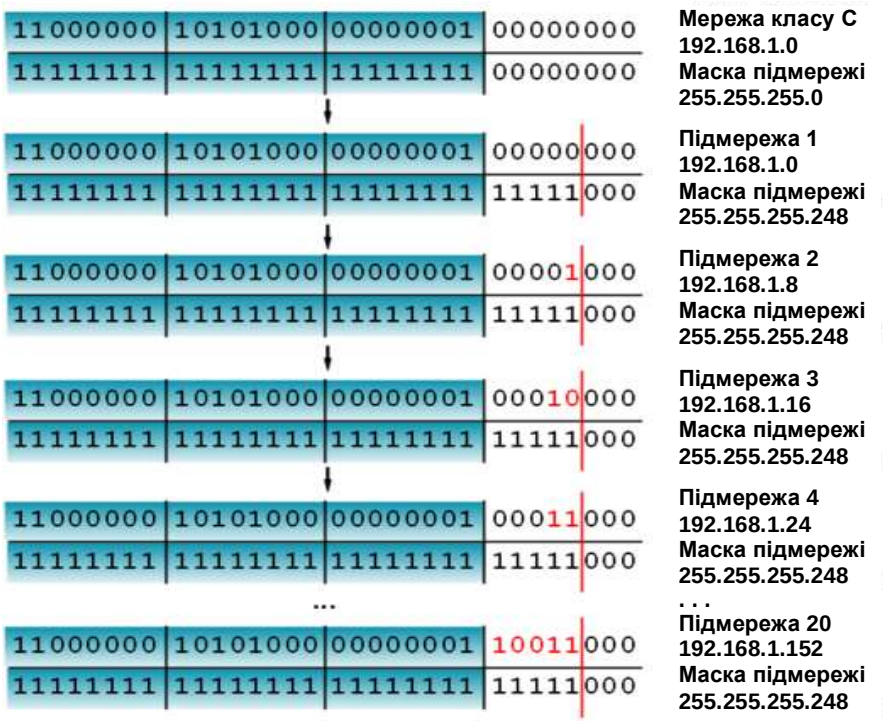


Рисунок 3.32 – Приклад розбивки мережі 192.168.1.0 на підмережі

3.3.3. Безкласове адресування

Класова модель IPv4-адресації виявилася нераціональної з погляду ефективного використання адресного простору. Навіть при використанні підмереж, у випадку класової адресації мереже можна було розбити тільки на підмережі однакового розміру. При цьому, якщо обрана маска підмережі забезпечує потрібну кількість підмереж, можливо, що припустимої кількості

вузлів для кожної підмережі буде недостатньо або, навпаки, частина адрес не буде використана. Наприклад, велика кількість вузлів є надлишковою для підмережі, яка зв'язує два маршрутизатори по каналу "точка-точка". У цьому випадку необхідно всього дві IPv4-адреси для адресації інтерфейсів сусідніх маршрутизаторів. Таким чином, розбивка мережі на підмережі різного розміру дозволила б раціонально використовувати адресний простір.

Поступово з ростом мережі Інтернет відбулася відмова від класової схеми, і була прийнята *безкласова модель IPv4-адресації*, у якій відсутня прив'язка до класу мережі й масці підмережі за замовчуванням. Безкласова адресація використовує *маски підмережі змінної довжини* (Variable Length Subnet Mask, VLSM) і *технологію безкласової міждоменої маршрутизації* (Classless Inter Domain Routing, CIDR). Термін «маска змінної довжини» означає, що мережа може бути розбита на підмережі з різними масками підмережі. Основна ідея застосування VLSM полягає в тому, що можна розбити мережу на підмережі, потім підмережі розбити ще на підмережі точно в такий же спосіб, як була розбита первісна мережа. Тобто мережа може бути розбита на підмережі різних розмірів, з різними масками. Маски підмережі є основою методу безкласової маршрутизації й записуються у вигляді нотації "IP-адреса/довжина префіксу". Число після "/" означає кількість одиничних розрядів у масці підмережі. Наприклад, мережна адреса 192.168.1.8 з маскою підмережі 255.255.255.248 також може бути записана, як 192.168.1.8/29. Число 29 указує, що в масці підмережі 255.255.255.248 є 29 одиничних біт.

Розподіл мережі на підмережі з використанням масок змінної довжини аналогічно традиційному розподілу на підмережі. Розглянемо приклад, показаний на рисунку 3.33.

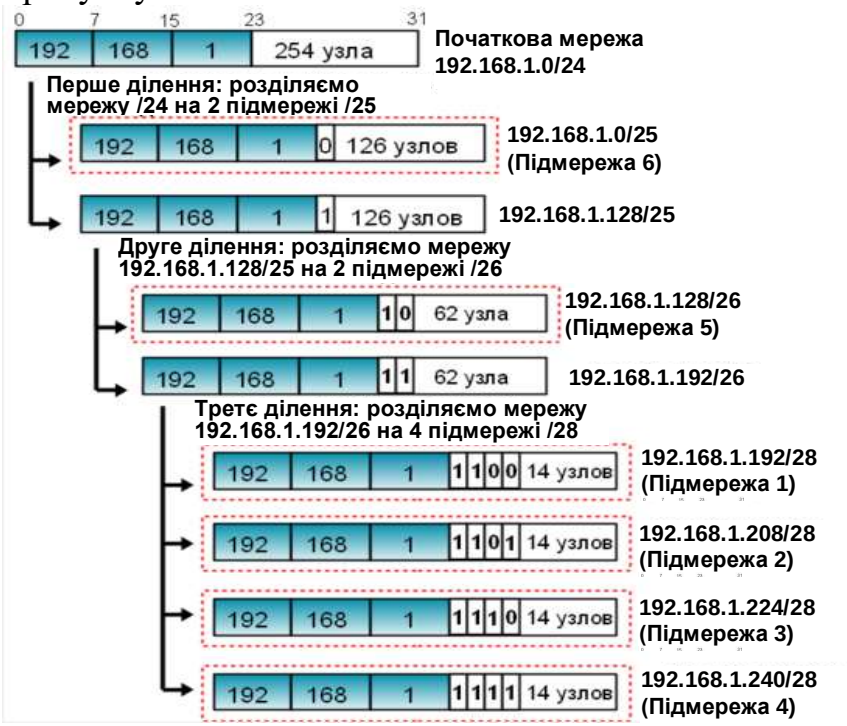


Рисунок 3.33 – Приклад розбивки мережі 192.168.1.0/24 на підмережі за допомогою VLSM

Припустимо організації виділена мережа класу C 192.168.1.0/24. Потрібно розділити її на 6 підмереж. У підмережах 1, 2, 3 і 4 повинне бути 10 вузлів, в 5-й підмережі – 50 вузлів, в 6-й підмережі – 100. Теоретично для мережі 192.168.1.0/24 припустима кількість вузлів дорівнює 254, і розбити таку мережу на підмережі з необхідною кількістю вузлів без використання VLSM неможливо.

Спочатку необхідно розділити мережу 192.168.1.0/24 на дві підмережі. Для цього з 4-го октету необхідно зайняти 1 біт для ідентифікатора підмережі, таким чином, для ідентифікації вузлів залишиться 7 біт. У підсумку виходить дві підмережі 192.168.1.0/25 і 192.168.1.128/25, у кожній з яких може бути по 126 (2^7–2) вузлів. Першу з них залишимо, тому що потрібно, щоб в 6-й підмережі було 100 вузлів, а другу розділимо ще на дві підмережі. Для цього заберемо 1 біт з тих 7 біт відведених під ідентифікатор вузла, що залишилися. Таким чином, виходить дві підмережі 192.168.1.128/26 і 192.168.1.192/26, у кожній з яких припустима кількість вузлів рівно 62 (2^6–2). Першу підмережу необхідно залишити для 5-й підмережі, у якій повинне бути 50 вузлів, а із другої підмережі сформувати ще чотири підмережі. Для цього займемо ще 2 біта з 6 біт, відведених під ідентифікатор вузла, що залишилися. У результаті одержимо чотири підмережі з 14 (2^4–2) вузлами в кожній, що дозволить адресувати необхідну кількість вузлів, необхідних для підмереж 1, 2, 3 і 4.

3.3.4. Порядок роботи протоколу DHCP

DHCP (англ. *Dynamic Host Configuration Protocol* – протокол динамічної конфігурації вузла) – це стандартний протокол прикладного рівня, який дозволяє комп'ютерам автоматично отримувати IP-адресу та інші параметри, необхідні для роботи в мережі. Для цього комп'ютер звертається до DHCP-сервера. Мережний адміністратор може задати діапазон адрес, які будуть розподілені між комп'ютерами. Це дозволяє уникнути ручного налаштування комп'ютерів мережі й зменшує кількість помилок. Протокол DHCP використовується в більшості великих мереж TCP/IP.

Крім IP-адреси, DHCP також може повідомляти клієнтові додаткові параметри, необхідні для нормальної роботи в мережі. Ці параметри називаються опціями DHCP. Список стандартних опцій можна знайти в RFC 2132. Деякими з найбільш часто використовуваних опцій є:

- IP-адреса маршрутизатора за замовчуванням;
- маска підмережі;
- адреси серверів DNS;
- ім'я домену DNS.

Деякі постачальники програмного забезпечення можуть визначати власні, додаткові опції DHCP.

Протокол DHCP працює за схемою клієнт-сервер. Під час запуску системи комп'ютер, який є DHCP-клієнтом, відправляє в мережу запит на отримання IP-адреси. DHCP-сервер відповідає і відправляє повідомлення-

відповідь, яка містить IP-адресу і деякі інші конфігураційні параметри. При цьому сервер DHCP може працювати в різних режимах, включаючи:

1. **Динамічний розподіл** - адміністратор присвоює IP-діапазон адрес на сервері DHCP. Кожен клієнтський комп'ютер в мережі повинен запросити IP-адресу від DHCP-сервера, коли мережа ініціалізується за концепцією "оренди". Коли закінчується термін оренди, якщо вона не буде продовжена, DHCP-сервер має право повернути адресу і призначити її на інші комп'ютери.
2. **Автоматичне виділення** - сервер DHCP буде постійно призначати вільний IP-адрес з діапазону, встановленого адміністратором, запитуючому комп'ютеру. Основна відмінність з динамічним розподілом в тому, що сервер зберігає записи минулих завдань IP і намагається привласнити ту ж адресу тому ж комп'ютеру для майбутніх мережних підключень.
3. **Статичний розподіл** - сервер DHCP робить призначення IP-адрес виключно на основі таблиці MAC-адрес, які зазвичай заповнені вручну адміністратором мережі. Якщо MAC-адреса комп'ютера не зазначена в таблиці, йому не буде призначена мережна адреса.

Протокол DHCP побудований так, що клієнт може звертатися із запитом відразу до декількох серверів.

Клієнт DHCP, що потребує адресу, посилає широкомовний пакет *DHCPDISCOVER* в пошуках сервера. Пакет містить апаратну адресу запитувача клієнта. Потім один або кілька серверів DHCP розглядають запит і посилають у відповідь пакет *DHCPOFFER*, що містить пропоновану IP-адресу і "час оренди".

Клієнт вибирає адресу з отриманих пакетів DHCPOFFER. Вибір клієнта залежить від його призначення - наприклад, він може вибрати адресу з найбільшим часом оренди. Слідом за тим клієнт посилає пакет *DHCPREQUEST* з адресою вибраного сервера.

Обраний сервер посилає підтвердження (*DHCPACK*) і процес узгодження завершується. Пакет DHCPACK містить обумовлені адресу та час оренди. Сервер позначає виділену адресу як зайняту - до закінчення терміну оренди цю адресу не можна буде присвоїти іншому клієнту. Клієнту залишилося тільки сконфігурувати себе відповідно до надісланих даних і можна приступати до роботи в мережі.

Отже, на запит DHCPDISCOVER може відповісти кілька серверів. Клієнт повинен вибрати одну з пропозицій і послати у відповідь пакет DHCPREQUEST з ідентифікатором вибраного сервера. Інші сервери переглядають пакет DHCPREQUEST і укладають на основі ідентифікатора сервера, що їх пропозиція була відкинута. Таким чином, вони знають, що запропоновані ними IP-адреси вільні для призначення іншим клієнтам.

У разі якщо сервер не може прийняти конфігурацію, він посилає пакет DHCPNAK (відмова в підтвердженні), що змушує клієнта почати процес узгодження заново. Виходячи з цього, якщо в мережі два DHCP-сервера з різними конфігураціями, немає ніякої гарантії, що клієнт вибере саме ваш сервер.

Якщо DHCP-сервер, розташований на віддаленому маршрутизаторі (R3), в іншій мережі і централізовано видає адреси в усі локальні мережі (LAN_1 і LAN_2), то необхідна конфігурація агентів DHCP-relay на маршрутизаторах, до яких підключені ці локальні мережі (R1 і R2) (рисунок 3.34). Сутність DHCP-relay полягає в пересиланні широкомовного пакету від клієнта одноадресним пакетом до DHCP-сервера.

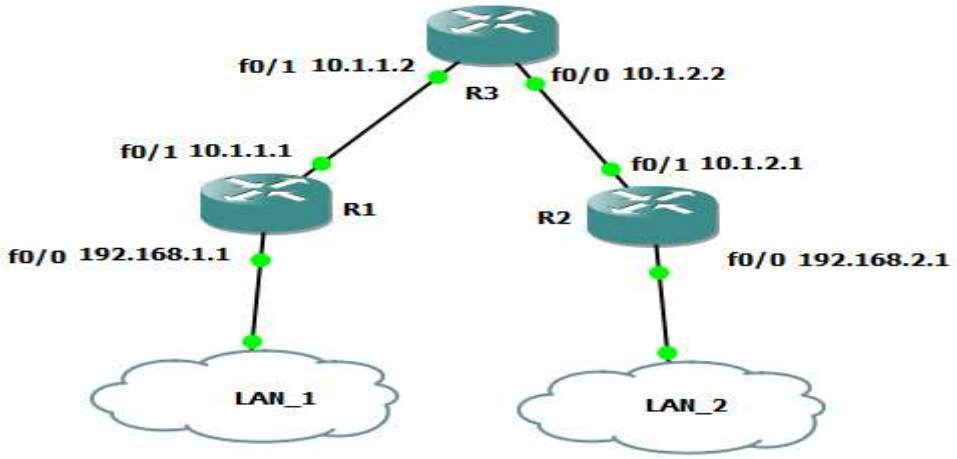


Рисунок 3.34 – DHCP-сервер, розташований на віддаленому маршрутизаторі

DHCPV6

SLAAC – це спосіб, який дозволяє пристрою отримати свій префікс, довжину префікса і адреса шлюзу від маршрутизатора IPv6 без допомоги DHCPv6-сервера. При використанні SLAAC для отримання необхідної інформації пристрої покладаються на повідомлення “Оголошення маршрутизатора ICMPv6”.

IPv6-маршрутизатори періодично відправляють повідомлення “Оголошення маршрутизатора ICMPv6” всіх пристроїв в мережі під управлінням IPv6. За замовчуванням маршрутизатори Cisco відправляють такі повідомлення кожні 200 секунд на адресу груповий передачі всім IPv6-вузлів. IPv6-пристрою, що знаходиться в мережі, не потрібно чекати цих періодичних повідомлень. Пристрій може відправити повідомлення “Запит маршрутизатора ICMPv6”, який використовує адресу груповий передачі всім IPv6-вузлів. Коли маршрутизатор IPv6 отримує таке повідомлення, він відразу ж відправляє у відповідь оголошення маршрутизатора.

IPv6-маршрутизація не включена за замовчуванням. Щоб маршрутизатор працював як IPv6-маршрутизатор, необхідно використовувати команду глобальної конфігурації ipv6 ***unicast-routing.***

Повідомлення “Оголошення маршрутизатора ICMPv6” містить префікс, довжину префікса і інші відомості IPv6-пристрої. Крім того, таке повідомлення вказує IPv6-пристрою, як йому отримати інформацію по адресації. повідомлення “Оголошення маршрутизатора” може виглядати в одному з наступних 3 варіантів:

– **Варіант 1:** ***тільки SLAAC***. Пристрій повинен використовувати префікс, довжину префікса і шлюз за замовчуванням, які містяться в повідомленні «Оголошення маршрутизатора». Інша інформація недоступна з DHCPv6-сервера.

– **Варіант 2:** ***SLAAC і DHCPv6***. Пристрій повинен використовувати префікс, довжину префікса і шлюз за замовчуванням, які містяться в повідомленні “Оголошення маршрутизатора”. На DHCPv6-сервері доступна і інша інформація, наприклад адресу DNS-сервера. Пристрій отримає цю додаткову інформацію в процесі пошуків і запитів до DHCPv6-сервера. Цей процес називається “DHCPv6 без запам’ятовування станів”, оскільки DHCPv6-сервери не виділяють і не відстежують будь-які призначення IPv6-адрес, а надають додаткову інформацію, наприклад про адресу DNS-сервера.

– **Варіант 3:** ***тільки DHCPv6*.** Пристрій не має використовувати інформацію з повідомлення “Оголошення маршрутизатора” для поповнення своєї інформації про адресації. Замість цього пристрій буде використовувати звичайні процеси пошуків і запитів до DHCPv6-серверів для отримання всієї своєї інформації про адресації. Така інформація включає в себе індивідуальну адресу IPv6, довжину префікса, адреса шлюзу та адреси DNS-серверів. В цьому випадку DHCPv6-сервер працює як DHCP-сервер, який фіксує дані аналогічно DHCP-сервера для IPv4. DHCPv6-сервер виділяє і відстежує IPv6-адреси, щоб не призначати один і той же IPv6-адреса на декількох пристроях.

3.4. Принципи керування мережами

3.4.1. Задачі систем управління телекомунікаційних та інформаційних мереж

Система мережного управління виконує завдання з надання адміністратору інформації про структуру мережі з усіма зв’язками, інформацію про стан керованих об’єктів (кінцевих вузлів, ліній зв’язку, інтерфейсів комунікаційної апаратури). Для рішення цієї задачі існують спеціалізовані пакети керуючого програмного забезпечення (ПЗ), як правило, орієнтовані на роботу з обладнанням одного виробника.

Це, наприклад, Transcend для обладнання 3Com, Optivity для Bay Networks, HP Open View для Hewelett-Packard, Spectrum для Cabletron, Nways Manager для IBM, LanDesk (управління робочими станціями) для Intel. Часто задачі управління вирішують в обмеженому обсязі, охоплюючи тільки комунікаційне обладнання, і не завжди в повному обсязі. Скорочення обсягу звичайно обумовлюється досить високою вартістю засобів управління.

Задачі мережного управління:

– *Вимір параметрів*, що визначають пропускну здатність, час відгуку, завантаження ліній і т.п. Система стежить за значеннями параметрів, визначає їхні середні (нормальні) значення, а по досягненні якими-небудь критичними параметрами заданих порогів генерує попередження чи автоматично виконує керуючі дії. Крім спостереження за мережею, у цій

області управління можливо й активний вплив на мережу за допомогою симуляторів (генераторів трафіку). Це допоможе оцінити поводження мережі при підвищенні навантаження (наприклад, при плануванні її розширення) і почати необхідні міри для забезпечення прийнятної продуктивності.

– *Відстеження інформації* про апаратні та програмні складові елементів вузлів мережі, включаючи дані про тип і версію продуктів, їх настройці і т.п. Сюди ж відноситься управління функціями пристроїв у цілому і конфігурування їхніх інтерфейсів.

– *Облік трафіку* окремих вузлів і їхніх груп як для ефективного розподілу ресурсів мережі, так і з метою визначення розміру оплати за надані послуги.

– *Виявлення і реєстрація відмов* для повідомлення адміністратора і відновлення працездатності. З появою симптомів відмови, система повинна по можливості ізолювати проблемну ділянку, задіяти резервні елементи, запротоколювати події, відновити вихідну конфігурацію після усунення відмовлень.

– *Управління доступом* до мережних ресурсів: авторизація користувачів, захист від несанкціонованого доступу, запобігання блокування мережі (навмисного і ненавмисного).

Для виконання цих завдань система управління виконує наступні ***функції***:

– Керування конфігурацією
– Керування якістю роботи
– Керування усуненням несправностей
– Керування розрахунками
– Керування безпекою

Керування конфігурацією передбачає:

– збір, ведення й відображення інформації про мережні елементи (їх типи, місцезнаходження, ідентифікатори й т.п.);
– уведення елементів в експлуатацію і їх вивід з експлуатації;
– установлення й зміна логічних з'єднань між елементами.

Керування якістю роботи:

– має на меті контроль і підтримку на необхідному рівні основних характеристик мережі

включає:

o збір, обробку, реєстрацію, зберігання й відображення статистичних даних про роботу мережі і її елементів;
o виявлення тенденцій у їхній поведінці й попередження про можливі порушення в роботі

Керування усуненням несправностей забезпечує:

– виявлення й локалізацію несправностей у мережі;
– реєстрацію несправностей і доведення відповідної до інформації до обслуговуючого персоналу;
– видачу рекомендацій з усунення несправностей.

Керування розрахунками:

- здійснює контроль над ступенем використання мережних ресурсів;
- підтримує функції по нарахуванню оплати за це використання.

Керування безпекою:

- забезпечує захист мережі від несанкціонованого доступу
- включає:
  - обмеження доступу за допомогою паролів;
  - видачу сигналів тривоги при спробах несанкціонованого доступу;
  - відключення небажаних користувачів;
  - криптографічний захист інформації керування.

Принципи побудови системи управління

Відносно систем управління мережами найбільш розробленим і ефективним для створення багаторівневої ієрархічної системи є стандарт Telecomunication Management Network (TMN), розроблений сумісно ITU-T (міжнародний союз електрозв'язку), ISO, ANSI і ETSI.

Незважаючи на те, що цей стандарт початково призначався для телекомунікаційних мереж (мереж зв'язку), орієнтація на використання загальних принципів зробила його корисним для побудови будь-якої інтегрованої системи управління мережами.

Стандарт TMN складається з великої кількості рекомендацій ITU-T і інших організацій стандартизації, а основні принципи моделі TMN приведені в рекомендації M.3010.

Модель TMN має 4 рівні:

1. Нижній рівень - **управління елементів мережі** (Network Element Layer – NEL) складається з окремих пристроїв мережі: КУА, підсилювачів, каналів, мультиплексорів, комутаторів, кінцевого обладнання і інших. Ці елементи мають вбудовані засоби для підтримки управління: датчики, інтерфейси управління. На сьогодні є пристрої, які крім загального стану контролюють ще й трафік, що проходити через елемент мережі. Подібні пристрої використовуються в технології FDDI, ISDN, Frame Relay, SDH.

Ці протоколи не маючи спеціального блоку управління зобов'язують пристрій підтримувати функції управління. Якщо ж немає встроєної функції управління тоді пристрої мережі мають окремі блоки управління, що підтримують один із двох найпоширеніших протоколів управління – SNMP (Simple Network Management Protocol) чи CMIP (Common Management Information Protocol) – інформаційний протокол загального управління.

Ці протоколи відносяться до прикладного рівня (7-го) моделі взаємодії відкритих систем (OSI).

2. **Рівень управління мережею** (Network Management Layer) – координує роботу елементарних систем управління елементами мережі. Дозволяє:

- контролювати конфігурацію каналів зв'язку,

- узгоджувати роботу транспортних підмереж різних технологій і т.д.

3. **Рівень управління послугами** (Servise Management Layer) – контроль і управління транспортними послугами і інформаційними послугами, що надаються користувачам. А також контроль результатів якості обслуговування (швидкість передачі в Frame Relay, пульсація пакетів і т.і.).

4. **Рівень адміністративного управління** (Buisiness Management Layer) – питання довгострокового планування мереж зі врахуванням фінансового і організаційного аспектів діяльності мережі. Отут автоматизована система управління підприємством виступає як аналог (прототип) системи управління.

Архітектура системи управління мережею зв'язку

Розподілена природа мереж обумовлює застосування моделі "менеджер-агент" для побудови системи управління (рисунок 3.35). *Менеджер* представляє собою програмно-апаратні засоби, що збирають інформацію від агентів, які виконують її обробку для надання адміністратору мережі. На підставі цієї інформації адміністратор за допомогою менеджера може здійснювати деякі керуючі впливи на об'єкти мережі. Управління може бути тією чи іншою мірою автоматизовано. *Агенти* розташовуються в керуємих елементах мережі. Вони безпосередньо взаємодіють з керованими об'єктами й обслуговують базу даних керованих параметрів (за якими ведеться спостереження). *Інформаційні бази управління* MIB (Management Information Base) містять списки керованих параметрів і їхнього значення, агенти відповідають за відповідність баз реальним станам об'єктів. Менеджер може в будь-який момент запросити інформацію про стан об'єкта, виконуючи операцію читання й агент у відповідь на цей запит зобов'язаний передати уміст усієї бази чи її частини. Операція запису в базу, якщо вона дозволена, змушує агента виконувати керуючі впливи на об'єкт. Опитування стану виконуються з ініціативи менеджера регулярно (полінг) чи епізодично, наприклад, по запиту адміністратора. Агенту можуть надаватися можливості й асинхронного повідомлення менеджера про настання яких-небудь подій. Для цього використовуються спеціальні повідомлення, названі *перериваннями* чи *тривогами* (trap, alert), що посилаються на адресу менеджера.

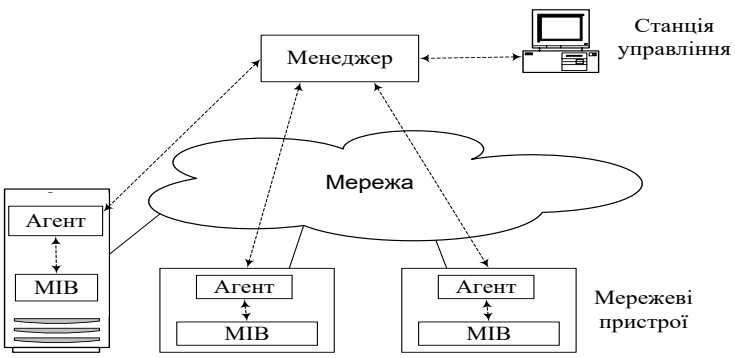


Рисунок 3.35 – Структура систем управління мережею

3.4.2. Реалізація задач маршрутизації в телекомунікаційних мережах

Процес вибору маршруту (шляху) переміщення повідомлень (пакетів) від джерела до адресату називають **маршрутизацією**.

Своєчасність і надійність доставки повідомлень (пакетів), а також завантаження комутаційних центрів (маршрутизаторів) в значній мірі визначаються ефективністю використовуваних алгоритмів маршрутизації.

В мережах з комутацією каналів алгоритм маршрутизації впливає лише на стадії установки з'єднання при виборі шляху (маршруту). В мережах з комутацією пакетів алгоритм маршрутизації може визначати шлях (маршрут) для кожного повідомлення (пакету) окремо, або ж серії повідомлень (пакетів).

По принципу пересування (передачі) повідомлень по маршруту від джерела до адресату виділяють методи **направленої** та **ненаправленої** маршрутизації.

Направлена маршрутизація – постійно забезпечує вибір оптимального маршруту у відповідності до прийнятого критерію передачі. З цією метою використовуються таблиці маршрутів, які формуються відповідними протоколами маршрутизації (динамічні маршрути), та за рахунок статичних маршрутів, які створює адміністратор мережі.

В свою чергу, *по способу формування таблиць маршрутів*, методи направленої маршрутизації діляться на **детерміновані (фіксовані)** та **адаптивні**.

Детермінований спосіб передбачає, що комутаційні центри мають фіксовані (статичні) таблиці маршрутів і передбачають єдиний шлях передачі для кожного напрямку зв'язку і не використовують який-небудь інший (на даний час) шлях передачі. Цей спосіб підходить для мереж з невеликим навантаженням.

Адаптивний спосіб надає можливість зміни шляху передачі в кожному комутаційному центрі (маршрутизаторі) в залежності від його завантаження і стану зв'язків.

Інформація, що необхідна для вибору шляху (маршруту) передачі в певний момент часу знаходиться:

– в попередньо складеній таблиці маршрутів комутаційного центру (маршрутизатору);

– відомостях про технічний стан вихідних каналів;

– довжинах черг, що очікують передачі на кожному з каналів.

Вибір оптимального маршруту здійснюється за допомогою розрахунків, що задовольняють умові передачі за визначеним критерієм.

Адаптивний спосіб може бути реалізований у вигляді:

– *локальної адаптивної маршрутизації*, яка для вибору шляху (маршруту) в кожному комутаційному центрі (маршрутизаторі) використовує лише відомості, що доступні на його рівні;

– *розподіленої адаптивної маршрутизації*, при якій маршрутна

інформація формується та розподіляється пристроєм, що реалізує функції централізованої маршрутизації.

Ненаправлена маршрутизація – немає систематичного алгоритму просування (передачі) повідомлення (пакету) по мережі. Такий спосіб маршрутизації може використовуватись в умовах відсутності даних про топологію мережі зв'язку. При цьому в комутаційних центрах відсутні таблиці маршрутів. *По способу формування маршрутів* методи ненаправленої маршрутизації діляться на **лавинні** або **випадкові**.

При **лавинному** способі повідомлення із комутаційних центрів (маршрутизаторів) передаються по всім напрямам підключеним до них, окрім каналу (інтерфейсу), по якому ці повідомлення надійшли на нього.

При **випадкової** маршрутизації повідомлення може бути передане на будь-який з вихідних каналів (інтерфейсів). При ненаправлених способах маршрутизації не потрібно знати топологію мережі. Таку маршрутизацію доцільно застосовувати в мережах з невеликим навантаженням і коли необхідна стійка робота мережі при виході з ладу різних її елементів.

В більшості випадків основним критерієм маршрутизації є використання найкоротших шляхів. Задачу про знаходження найкоротшого шляху можна сформулювати в наступному вигляді. Дано зв'язану мережу *G*, у якій кожній дузі (ребру) приписано вагу, пропорційну до її (його) довжини. Потрібно знайти шлях μ_{st} між заданими вершинами *s* та *t*, який має мінімально можливу довжину, тобто:

$$l = \sum_{(i,j)\in\mu_{st}} m_{ij} \rightarrow \min(\text{на } \mu')$$

де μ' – множина всіх можливих шляхів з *s* до *t*.

Процедуру маршрутизації доцільно розрізняти в межах однієї локальної мережі і міжмережну. Для реалізації процесу маршрутизації в локальній мережі важлива функція покладена на протокол ARP.

ARP (англ. *Address Resolution Protocol* – протокол визначення адрес) – комунікаційний протокол, призначений для перетворення IP-адрес в MAC-адреси (адреси канального рівня) в мережах TCP/IP.

ARP-таблиця для перетворення адрес

Перетворення адрес виконується шляхом пошуку за таблицею. Ця таблиця називається ARP-таблицею, зберігається у пам'яті й містить рядки для кожного вузла мережі. В двох стовпчиках містяться IP- та MAC-адреси. Якщо потрібно перетворити IP-адресу в Ethernet-адресу, то відбувається пошук запису з відповідною IP-адресою. Нижче наведено приклад спрощеної ARP-таблиці (таблиця 3.5).

ARP-таблиця необхідна через те, що IP-адреси та MAC-адреси вибираються незалежно, і немає жодного алгоритму для перетворення однієї в іншу. IP-адресу вибирає менеджер мережі з урахуванням розташування

машини у мережі Інтернет. Якщо машину переміщують до іншої частини мережі Інтернет, то її IP-адреса повинна бути змінена. MAC-адресу вибирає виробник мережного інтерфейсного обладнання з виділеного для нього згідно з ліцензією адресного простору. Якщо в машини змінюється мережний адаптер, то змінюється й MAC-адреса.

Таблиця 3.5 – Приклад ARP-таблиці

IP-адреса	**Ethernet-адреса**
223.1.2.1	08:00:39:00:2F:C3
223.1.2.2	08:00:5A:21:A7:22
223.1.2.3	08:00:10:99:AC:54

Порядок перетворення адрес

У ході звичайної роботи мережна програма відправляє прикладне повідомлення, користуючись транспортними послугами TCP. Модуль TCP надсилає відповідне транспортне повідомлення через модуль IP. У результаті складається IP-пакет, який має передаватись драйверові Ethernet. IP-адреса місця призначення відома прикладній програмі, модулеві TCP та модулеві IP. Необхідно на її основі знайти MAC-адресу місця призначення. Для пошуку відповідної MAC-адреси використовується ARP-таблиця.

Запити та відповіді протоколу ARP

ARP-таблиця заповнюється автоматично модулем ARP по мірі отримання вузлом відповідної інформації. Коли за допомогою існуючої ARP-таблиці не вдається перетворити IP-адресу, то відбувається наступний процес:

1. По мережі передається широкомовний ARP-запит.
2. Вихідний IP-пакет ставиться в чергу.

Кожний мережний адаптер приймає широкомовні передачі. Усі драйвери Ethernet перевіряють поле типу в прийнятому Ethernet-кадрі й передають ARP-пакети модулю ARP. ARP-запит можна інтерпретувати так: “Якщо ваша IP-адреса збігається із зазначеною, то повідомте мені вашу Ethernet-адресу”. Пакет ARP-запиту виглядає приблизно як таблиця 3.6.

Таблиця 3.6 – Приклад ARP-запиту

IP-адреса відправника	223.1.2.1
MAC-адреса відправника	08:00:5A:21:A7:22
Шукана IP-адреса	223.1.2.3
Шукана MAC-адреса	<порожньо>

Кожний модуль ARP перевіряє поле шуканої IP-адреси в отриманому ARP-пакеті і, якщо адреса збігається з його власною IP-адресою, то посилає

відповідь прямо на MAC-адресу відправника запиту. Пакет з ARP-відповіддю виглядає приблизно як таблиця 3.7.

Таблиця 3.7 – Приклад ARP-відповіді

IP-адреса відправника	223.1.2.3
MAC-адреса відправника	08:01:2A:2B:A7:21
IP-адреса автора запиту	223.1.2.1
MAC-адреса автора запиту	08:00:5A:21:A7:22

Цю відповідь одержує вузол, що зробив ARP-запит. Мережна карта цього вузла перевіряє поле типу повідомлення в Ethernet-кадрі й передає ARP-пакет модулю ARP. Модуль ARP аналізує ARP-пакет і додає запис у свою ARP-таблицю. Якщо в мережі немає вузла із шуканою IP-адресою, то ARP-відповіді не буде й не буде запису в ARP-таблиці. Протокол IP буде знищувати IP-пакети, що направляються по цій адресі. Протоколи верхнього рівня не можуть відрізнити випадок пошкодження мережі Ethernet від випадку відсутності вузла із шуканою IP-адресою.

Статична маршрутизація має ряд переваг в порівнянні динамічної маршрутизацією, в тому числі:

– .

– Статичні маршрути створюють менше навантаження на пропускну здатність, ніж протоколи динамічної маршрутизації, і для розрахунку і для передачі даних про маршрути не використовуються ресурси центрального процесора.

– Шлях, який використовується статичним маршрутом для відправки даних, буде відомий.

Наступний перехід може бути визначений за IP-адресою, інтерфейсу виходу або по обох параметрах разом (рисунок 3.36).

```
Router(config)# ip route network-address subnet-mask
{ip-address | exit-intf}
```

Рисунок 3.36 – Налаштування статичного маршруту

– *Маршрут наступного переходу*. Вказується лише IP-адреса наступного переходу.

– *Безпосередньо підключений статичний маршрут.* Вказується лише інтерфейс виходу маршрутизатора.

– *Повністю заданий статичний маршрут.* Визначено IP-адреса і інтерфейс виходу наступного переходу.

– *Безпосередньо підключений статичний маршрут*. Вказується лише інтерфейс виходу маршрутизатора.

–

Статичний маршрут «за замовчуванням» – маршрут, що визначає IP-адресу шлюзу, на який маршрутизатор відправляє всі IP-пакети, для яких у нього немає динамічного або статичного маршруту (рисунок 3.37).

```
Router(config)#ip route 0.0.0.0 0.0.0.0 {ip-address | exit-intf}
```

Рисунок 3.37 – Налаштування маршруту «за замовчуванням»

Адміністративна відстань для ***"плаваючих статичних маршрутів"*** більше, ніж адміністративна відстань іншого статичного маршруту або динамічних маршрутів. Статичний маршрут «плаває» і не використовується, коли активний маршрут з меншою адміністративною відстанню (рисунок 3.38).

```
R1(config)# ip route 0.0.0.0 0.0.0.0 172.16.2.2
R1(config)# ip route 0.0.0.0 0.0.0.0 10.10.10.2 5
R1(config)#
```

Рисунок 3.38 – Налаштування «плаваючого» маршруту «за замовченням»

3.4.3. Таблиці маршрутизації та порядок їх складання

Таблиця маршрутизації є для маршрутизатора керівним документом, яким чином діяти з певними пакетами. що надходять на нього, і зберігає інформацію про:

- ***Маршрути із прямим підключенням*** – це маршрути, що прямо надходять із активних інтерфейсів маршрутизатора (підключені до нього).
- ***Вилучені маршрути*** – це маршрути до вилучених мереж, підключених до інших маршрутизаторів.

Таблиця маршрутизації являє собою файл даних в ОЗУ, що зберігає інструкції для маршрутизатора – як досягти конкретного місця призначення, куди конкретно відправити пакет, на який наступний перехід на шляху до пункту призначення.

На маршрутизаторі Cisco IOS команда **show ip route** може бути використана для відображення таблиці IPv4-маршрутизації (рисунок 3.39).

У таблиці маршрутизації можуть бути такі види записів:

– ***локальні маршрути*** **–** додаються, коли інтерфейс настроєний і активний, указує адресу, призначену інтерфейсу маршрутизатора (**L**).

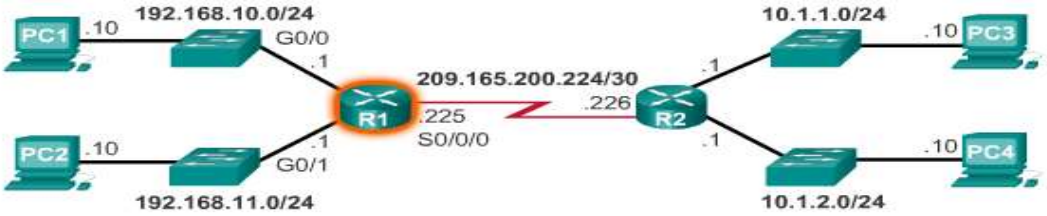
– ***прямі підключення*** **–** визначає мережу із прямим підключенням (**C**).

– ***статичні маршрути*** – додаються, коли маршрут настроєний вручну адміністратором (**S**).

– ***динамічні маршрути*** **–** додаються, коли визначені мережі й реалізуються протоколи маршрутизації, які одержують інформацію про мережу динамічно (**R**, **D**, **O**…).

Кожний запис в таблиці містить наступні відомості (рисунок 3.40):

- **Джерело маршруту –** визначення способу одержання маршруту.
- **Мережа призначення** – визначення адреси вилученої мережі.
- **Адміністративна відстань –** визначення надійності джерела маршруту. Низькі значення вказують на краще джерело маршруту (таблиця 3.8).
- **Метрика –** визначення значення, привласненого для досягнення вилученої мережі. Низькі значення вказують на кращі маршрути.
- **Наступний перехід –** визначення IPv4-адреси наступного маршрутизатора, на який слід переслати пакет.
- **Часова мітка маршруту –** визначення кількості часу, що пройшов з тих пор, як був отриманий маршрут.
- **Вихідний інтерфейс –** визначення вихідного інтерфейсу для відправлення пакета до кінцевого пункту призначення.




```
Gateway of last resort is not set
     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
D       10.1.1.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
D       10.1.2.0/24 [90/2170112] via 209.165.200.226, 00:00:05,
        Serial0/0/0
     192.168.10.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.10.0/24 is directly connected, GigabitEthernet0/0
L       192.168.10.1/32 is directly connected, GigabitEthernet0/0
     192.168.11.0/24 is variably subnetted, 2 subnets, 3 masks
C       192.168.11.0/24 is directly connected, GigabitEthernet0/1
L       192.168.11.1/32 is directly connected, GigabitEthernet0/1
```

Рисунок 3.39 – Таблиця маршрутизації

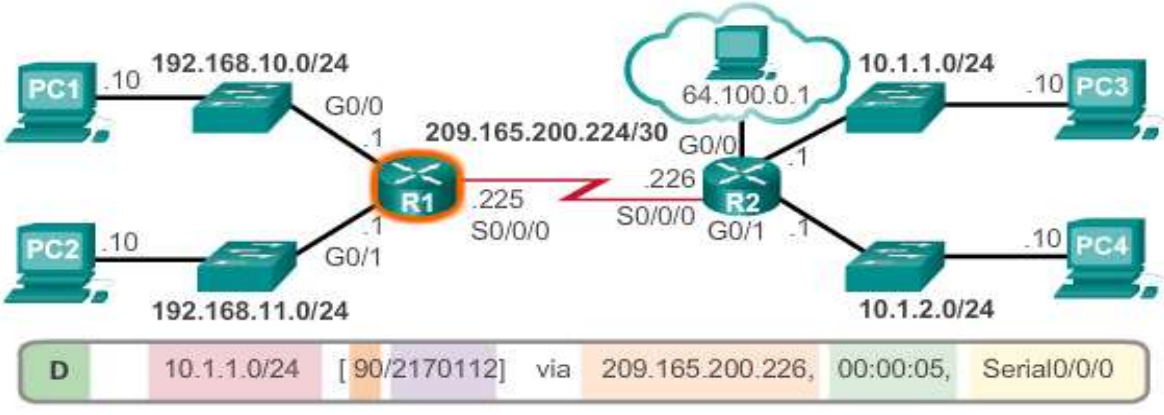


Рисунок 3.40 – Записи в таблиці маршрутизації

Таблиця 3.8 – Припустимі значення адміністративної відстані

Route Source	Administrative Distance
Connected	0
Static	1
EIGRP summary route	5
External BGP	20
Internal EIGRP	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
External EIGRP	170
Internal BGP	200

3.4.4. Огляд основних протоколів маршрутизації

Протокол маршрутизації RIP

RIP (Routing Information Protocol) – один з перших протоколів внутрішньої маршрутизації, що застосовувалися в Інтернеті (1982 р.). Перша версія протоколу RIP описана в специфікації RFC 1058, а друга (RIP ver. 2) – в специфікації RFC 2453. В цьому протоколі метрикою є кількість пересилань між вузлами (*hops*). Ця метрика не забезпечує облік пропускної здатності, надійності та завантаженості трактів передачі, а також характеристик трафіка користувачів.

RIP – це протокол дистанційно-векторної маршрутизації, що ґрунтується на використанні вектору відстаней (*Distance Vector*). Він не дозволяє забезпечити функціонування широкомасштабних мереж через обмеженість числа пересилань (*hops*) до 15.

Робота протоколу RIP заснована на широкомовному розсиланні повідомлень про коректування маршрутів. Періодичність розсилання оновлень – 30 с. Розсилаються повні копії таблиць маршрутизації кожного маршрутизатора незалежно від того, змінені вони чи ні.

Протокол маршрутизації OSPF

Протокол OSPF (Open Shortest Path First) належить до класу протоколів стану каналів (Link State Protocol). Дослівний переклад – першим обирається найкоротший шлях (використовує алгоритм Дейкстри).

В OSPF підтримуються метрики пропускної здатності та затримки. Метрика, що оцінює пропускну здатність каналу, визначається, наприклад, обладнанням компанії Cisco, як кількість секунд, необхідних для передачі 100 Мбіт.

Повідомлення OSPF інкапсулюється прямо в IP пакет (поле даних), тобто протоколи транспортного рівня не використовуються.

Основні гідності OSPF.

- Відсутність обмеження на розмір мережі.
- Автономна система може бути поділена на області маршрутизації.
- Висока швидкість встановлення маршрутів.

Протокол пограничного шлюзу BGP

Завдання BGP – побудова маршрутів між мережами, що належать різним автономним системам. Протокол BGP на основі інформації, отриманої від різних маршрутизаторів, вибудовує граф автономних систем (АС) з усіма зв'язками між вузлами. Такий граф іноді називають деревом. Якщо розглядати мережу Internet "очима" протоколу BGP, то це буде граф, що складається з автономних систем, де кожній автономній системі відповідає свій унікальний номер. З'єднання між двома автономними системами формує шлях, а інформація про сукупність шляхів від одного вузла в автономній системі до вузла в іншій автономній системі становить маршрут. Протокол BGP активно використовує інформацію про маршрути до заданого пункту призначення, що дозволяє уникнути утворення петель маршрутизації між доменами.

В основі протоколу BGP лежать оголошення про маршрути. Оголошення про маршрути посилає один рівноправний BGP-вузол іншому рівноправному BGP-вузлу для з'єднання "точка-точка". Оголошення складається з адреси мережі (наприклад, 10.1.10/24) і набору атрибутів, асоційованих з маршрутом до цієї мережі. Двома найбільш важливими атрибутами є атрибут маршруту (явний список усіх автономних систем на шляху до зазначеної мережі) і ідентифікатор наступного маршрутизатора на шляху до зазначеної мережі призначення. Таким чином, формується ієрархічна схема маршрутизації, що зв'язує різні вузли й автономні системи в єдину мережу.

Очевидно, що BGP-маршрутизатори, що перебувають в одній АС, також повинні обмінюватися між собою маршрутною інформацією. Це необхідно для погодженого відбору зовнішніх маршрутів відповідно до політики даною АС і для передачі транзитних маршрутів через автономну систему. Такий обмін проводиться також по протоколу BGP, який у цьому випадку часто називається *IBGP* (*Internal BGP-внутрішній протокол* BGP), відповідно, протокол обміну маршрутами між маршрутизаторами різних АС називають зовнішнім протоколом BGP і позначають *EBGP* (*external BGP*).

Крім того існують протоколи EIGRP, IS-IS і т.д.

Контрольні питання до розділу 3

1. Опишіть принципи та технології комутації.
2. Дайте визначення локальної мережі, охарактеризуйте основні види структур.
3. Охарактеризуйте множинний доступ з опитуванням каналу і виявленням конфліктів – CSMA/CD. Особливості CSMA/CA.
4. Поясніть поняття IP-адрес і їх масок, способи задання масок.
5. Надати характеристику операційної системи IOS (режими і їх призначення).

РОЗДІЛ 4
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ТЕЛЕКОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

4.1. Технології мереж доступу xdsl та xpon

4.1.1. Поняття систем абонентського доступу

У зв'язку з якісними змінами, що відбуваються в розвитку сучасних телекомунікаційних мереж, і зокрема зі створенням мультисервісних мереж, здійснюється впровадження сучасних технологій і на абонентських мережах доступу. На рисунку 4.1 показаний фрагмент телекомунікаційної мережі з виділеними типовими елементами мереж доступу.

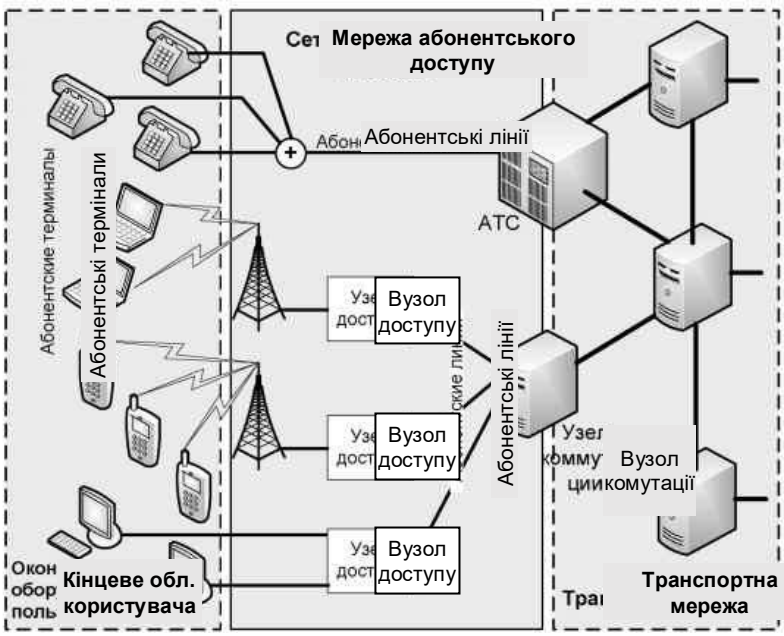


Рисунок 4.1 – Типова структура й состав мереж абонентського доступу

Абонентська мережа в найпростішому випадку складається із трьох основних елементів:

- абонентського (користувацького) термінала;
- абонентської (користувацької) лінії (АЛ);
- частини елементів вузла комутації.

Проблему абонентського доступу до послуг телекомунікаційної мережі на ділянці "абонентський термінал-вузол доступу" з той же якістю, що й безпосередньо в телекомунікаційній мережі, прийнято називати проблемою "останньої милі".

Мережі абонентського доступу з малою пропускною здатністю перестали забезпечувати зростаючі потреби користувачів. Тому в багатьох країнах світу побудова високошвидкісних, тобто широкосмугових, мереж доступу стало пріоритетним напрямком їх розвитку.

Спеціальні технології абонентського доступу насамперед націлені на утворення цифрових каналів на основі доступного фізичного середовища, різновиди якої можна розділити на дві групи:

1. Фізичні середовища дротового доступу:

– оптичне волокно;
– коаксіальний мідний кабель;
– симетричний мідний кабель.

2. Фізичні середовища бездротового доступу:

– оптичні електромагнітні хвилі;
– радіохвилі.

У цей час намітилися три найбільш характерні шляхи вирішення проблеми «останньої милі».

1. *Будівництво волоконно-оптичних ліній зв'язку* (ВОЛЗ) на ділянці «останньої милі» має ряд очевидних переваг і відповідає перспективним концепціям. Вартість оптичного кабелю (ОК) неухильно знижується, причому оптичні АЛ служать досить довго й не вимагають особливої уваги. Однак для прокладки кабелю необхідні трудові й часові витрати спеціально підготовлених працівників, а також недешеве кінцеве встаткування приймання/передачі й мультиплексування, що збільшує вартість АЛ.

2. *Ущільнення існуючих (мідно-кабельних) абонентських ліній*. Ідея ущільнення АЛ народилася давно. Аналогове встаткування високочастотного ущільнення широко використовується в телекомунікаційних мережах дотепер. Однак своїм справжнім розвитком даний напрямок зобов'язаний появі цифрових абонентських ліній ЦАЛ (DSL – Digital Subscriber Loop або Line). Технології xDSL (де x – узагальнений символ різних абревіатур, відповідних до різних варіантів DSL) дозволили організувати високошвидкісну цифрову передачу по існуючим АЛ.

Додатковим резервом побудови систем абонентського доступу на базі існуючих дротових "абонентських ліній" служать:

– лінії електропередач (наприклад, відомі технології X.10 і DPL – Digital Power line, які дозволяють передавати дані по електропроводці зі швидкістю до 1 Мбіт/с і інші);
– мережі кабельного телебачення.

3. Використання *технологій бездротового абонентського доступу*. Останнім часом значно зріс інтерес до технологій бездротового абонентського доступу, іменованим WLL-технологіями (Wireless Local Loop).

Технології бездротового абонентського доступу мають безперечні переваги перед провідними:

– застосування в місцях відсутності кабельної інфраструктури, а також у важкодоступних і малонаселених районах;
– швидке розгортання й уведення в експлуатацію;
– організація доступу в будь-якому місці (у межах зон покриття);
– підтримка зв'язку абонентів в русі.

Головні недоліки WLL – обмежена пропускна здатність і відносно висока вартість розраховуючи на одного абонента, а також традиційні для радіозв'язку проблеми "відкритості" до зовнішніх впливів.

У цей час існує величезну безліч WLL-технологій, які умовно розділяються на дві більші групи:

- фіксованого зв'язку;
- рухомого зв'язку.

4.1.2. Класифікація та реалізація систем доступу технології xDSL

DSL (Digital Subscriber Line) – технології надання користувачам телефонних мереж загального користування (ТФЗК) послуг мультимедіа, що використовують у якості середовища передачі існуючу інфраструктуру ТФЗК.

Поповнюване сімейство технологій DSL є досить новим і дозволяє ефективно використовувати смугу пропускання мідних телефонних ліній. Розширити смугу пропускання від 4 кГц (як це було в традиційній аналоговій телефонії) виявилося реальним за допомогою спеціальних лінійних кодів і техніки цифрових сигнальних процесорів. Технології DSL використовують різні схеми багатопозиційного лінійного кодування: CAP, 2B1Q, PAM і ін. Класифікація технологій xDSL представлена на рисунку 4.2.

Технології симетричного DSL-доступу використовуються при наданні послуг об'єднання LAN, організації виносів, підключенні встаткування користувача до транспортних мереж по симетричних мідних лініях. До цієї групи відносяться технології: HDSL, SDSL, MDSL, MSDSL, SHDSL, HDSL 2/4 і VDSL.

Симетричні технології xDSL розрізняють по числу пар використовуваних проводів.

Спочатку з'явився варіант HDSL для двох пар, який використовує кодування 2B1Q. Потім пройшла стандартизація HDSL для трьох, двох і однієї пар з використанням 2B1Q або CAP. Часто вживаються позначення HDSL2 і SDSL2, причому технологія HDSL2 розрахована винятково на передачу Tl, а SDSL2 підтримує швидкості від 384 кбіт/с до 2,304 Мбіт/с (із кроком 64 кбіт/с).

Системи SHDSL здатні працювати по одній або по двом крученим парам зі швидкістю передачі відповідно від 192 до 2312 кбіт/с із кроком 8 кбіт/с і від 384 до 4624 кбіт/с із кроком 16 кбіт/с.

Потім були розроблені асиметричні системи – ADSL (так звана Full-rate DSL). Технологія забезпечує максимальну швидкість передачі в прямому напрямку – 6,144 Мбіт/с, а у зворотному – 0,640 Мбіт/с.

Перші лінії ADSL припускали роботу тільки на постійних швидкостях. Тим часом сучасні розв'язки ADSL можуть регулювати швидкість передачі залежно від якості лінії. Через адаптивність швидкості передачі цю технологію іноді називають RADSL (Rate Adaptive DSL).

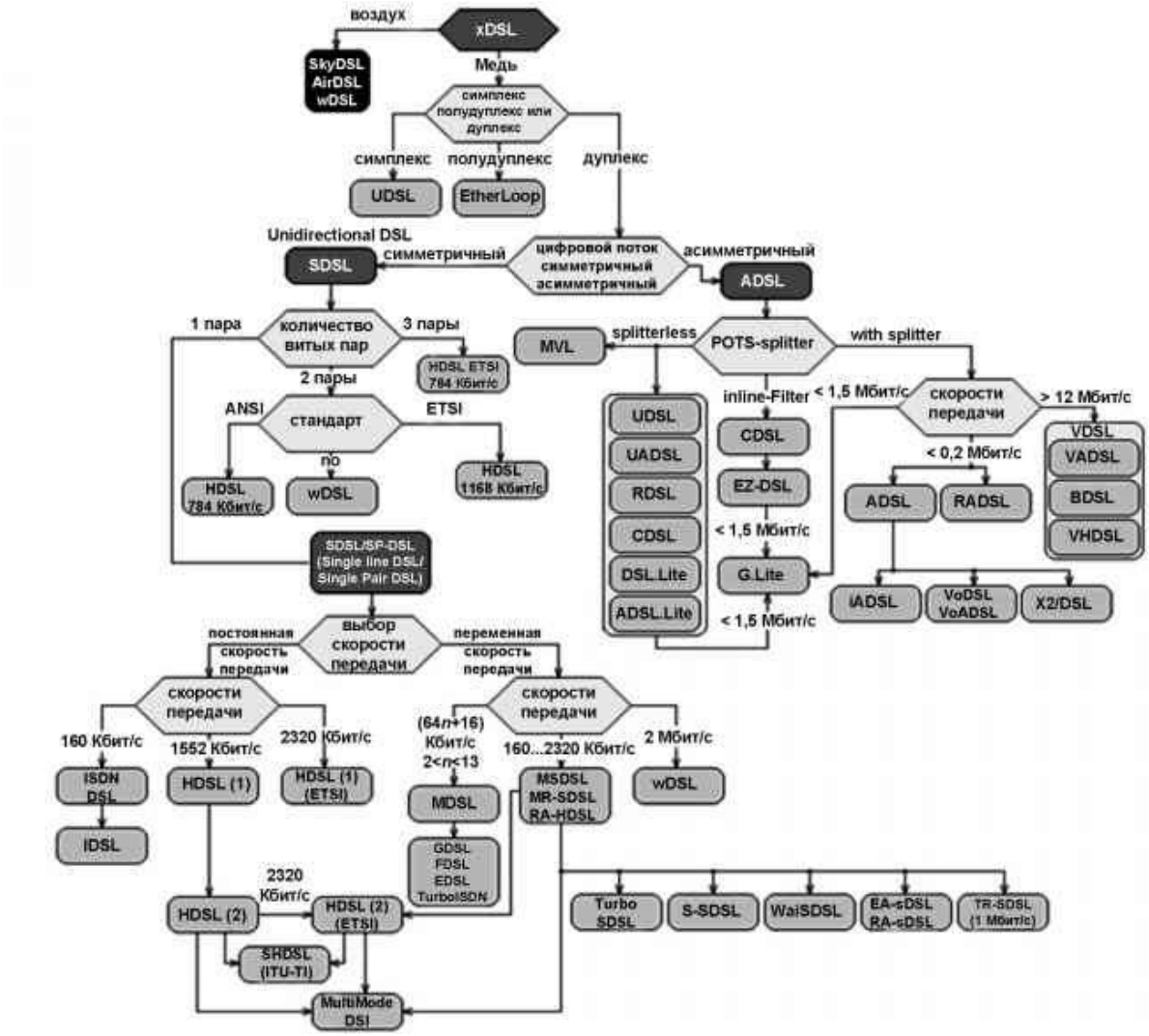


Рисунок 4.2 – Класифікація xDSL

Дуже високі швидкості передачі в прямому й зворотному напрямках досягаються за допомогою VDSL. Раніше для VDSL використовувалися також позначення VADSL, BDSL (Broadband DSL) або VHDSL (Very High bitrate DSL).

Впровадження ADSL на практиці показало, що установка розгалужувачів пов’язана з більшими витратами, тому були початі пошуки технологій ADSL без розгалужувача. Цілим рядом фірм були запропоновані різні варіанти, виходячи зі зменшення швидкості передачі в обох напрямках у порівнянні з ADSL (наприклад, MVL – Multiple virtual Line DSL, CDSL – Consumer DSL, CiDSL – Consumer installable DSL).

Одним із самих популярних останнім часом є термін – VoDSL (Voice over DSL), що буквально означає передачу мовних сигналів по цифрових лініях мережі абонентського доступу. У цілому дане позначення підходить майже до всіх високошвидкісних технологій xDSL. Окремо виділяють VoSDSL і VoADSL, особливістю яких є комбінація стиску мовних сигналів і ATM.

Розвиток технологій цифрової обробки сигналу (DSP) у комбінації з новітніми алгоритмами й технологіями кодування дозволили підняти

інформаційну ємність мереж доступу до 55 Мбіт/с (рисунок 4.3). Завдяки різноманіттю xDSL користувач може вибрати для себе підходящий варіант по швидкості приймання/передачі даних - від 32 кбіт/с до більш ніж 50 Мбіт/с. І в першу чергу вибір буде ґрунтуватися на типі й кількості наявних у користувача пар, їх якості й довжини.

У цей час найбільше поширення у світовій практиці одержали наступні різновиди технології xDSL:

– ADSL – асиметрична цифрова абонентська лінія;
– HDSL – швидкісна цифрова абонентська лінія;
– MDSL – середньошвидкісна цифрова абонентська лінія;
– VDSL – високошвидкісна цифрова абонентська лінія;
– RA-HDSL – цифрова абонентська лінія зі східчастим регулюванням швидкості;
– SDSL – симетрична абонентська лінія, що працює по одній парі;
– SHDSL – симетрична високошвидкісна абонентська лінія, що працює по одній парі;
– IDSL – цифрова абонентська лінія для однієї пари проводів, використовуваної для передачі сигналів ISDN.

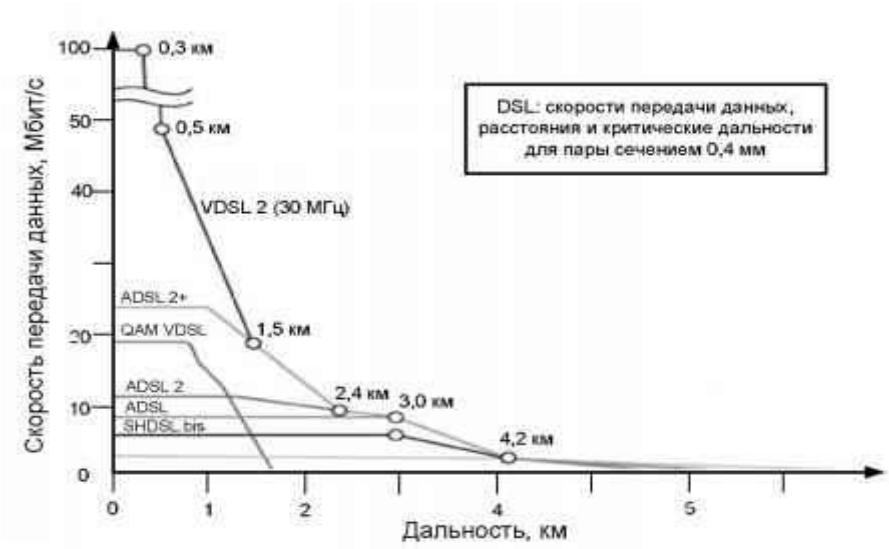


Рисунок 4.3 – Залежність швидкості передачі даних від відстані для пари перетином 0,4 мм (за даними компанії Zyxel)

Докладні технічні характеристики окремих технологій DSL, а також їх типове застосування наведені в таблицях 4.1 і 4.2.

Найбільшого практичного поширення отримали асиметричні системи DSL. Асиметрія швидкості передавання від абонента та до нього, у комбінації зі станом “постійно встановленого з’єднання” (коли виключається необхідність щораз набирати телефонний номер і чекати установки з’єднання), робить технологію ADSL ідеальної для організації доступу в мережу Інтернет, доступу до локальних мереж (ЛВС) і т.п. При організації таких з’єднань користувачі звичайно одержують набагато більший обсяг інформації, чим передають.

Таблиця 4.1 – Порівняння можливостей найбільш значимих xDSL

Критерій	G.SHDSL	ADSL	ADSL2	ADSL2+	ADSL2++	VDSL
Число пар у лінії	до 4	1	1	1	1	до 2
Довжина лінії перетином 0,4 мм, км	до 6 без регенерації, до n×6 з регенерацією	5	5	5	5	до 1,2 по 1 парі до 2 по 2 парах
Максимальна швидкість (до абонента/ від абонента), Мбіт/с	2,3 по 1 парі 4,6 по 2 парах	8/1	12/1	24/2	48/3	18/16 (QAM) 50/30 (DMT)
Робота «поверх» телефонної лінії	немає	так	так	так	так	так
Регенерація	Тільки для цифрових потоків	немає	немає	немає	немає	немає
Можливість роботи модему «один на одного»	так	немає	немає	немає	немає	так

Технологія ADSL забезпечує швидкість “спадного” потоку даних у межах від 1,5 до 48 Мбіт/с і швидкість «висхідного» потоку даних від 640 кбіт/с до 3 Мбіт/с. ADSL дозволяє передавати дані на відстань до 5,5 км по одній крученій парі проводів діаметром 0,5 мм.

ADSL дозволяє використовувати ту ж саму пару проводів для традиційного телефонного зв’язку. Для цього використовуються спеціальні пристрої поділу сигналів (сплітери) – рисунок 4.4.

Рисунок 4.4 – Концепція асиметричної цифрової абонентської лінії (ADSL)

ADSL використовує технологію FDD (частотний поділ для забезпечення дуплексного зв’язку), яка дозволяє виділити одну смугу частот для висхідного потоку даних (напрямок від користувача до станції), а іншу смугу частот – для спадного потоку даних (від станції до користувача) – рисунок 4.5.

Таблиця 4.2 – Типове застосування окремих технологій DSL

Технологія DSL	Тип передачі Максимальна швидкість (приймання/ передача)	Max відстань	Кількість телефонних пар	Основне застосування
ADSL	Асиметричний 24 Мбіт/с /3,5 Мбіт/с	5,5 км	1	Доступ в Інтернет, голос, відео, HDTV (ADSL2+)
IDSL	Симетричний 144 кбіт/с	5,5 км	1	Передача даних
HDSL	Симетричний 1,544...2,048 Мбіт/с	4,5 км	1,2	Об’єднання мереж, послуги E1
SDSL	Симетричний 2 Мбіт/с	3 км	1	Об’єднання мереж, послуги E1
VDSL	Асиметричний 62 Мбіт/с / 26 Мбіт/с	1,3 км на шах. швидкості	1	Об’єднання мереж, HDTV
SHDSL	Симетричний 2,32 Мбіт/с	до 7,5 км	1	Об’єднання мереж
UADSL	Асиметричний 1,5 Мбіт/с /384 кбіт/с	3,5 км на шах. швидкості	1	Доступ в Інтернет, голос, відео
RADSL	Асиметричний 8 Мбіт/с / 640 кбіт/с	3-5 км залежно від діаметра проводу		
MDSL	Діапазон може бути в будь-якій пропорції розділений між спадним і висхідним трафіком 768 кбіт/с	3-5 км залежно від діаметра проводу		

Устаткування ADSL, розміщене на АТС, і абонентський ADSL-модем, що підключаються до обох кінців телефонної лінії, утворюють три групи каналів (три піддіапазони) передачі даних і телефонії:

– високошвидкісну з мережі до абонента (швидкість – від 32 кбіт/с до 48 Мбіт/с);

– швидкісну від абонента в мережу (швидкість – від 32 кбіт/с до 3 Мбіт/с);

– простий канал телефонного зв’язку, по якому передаються звичайні телефонні розмови.

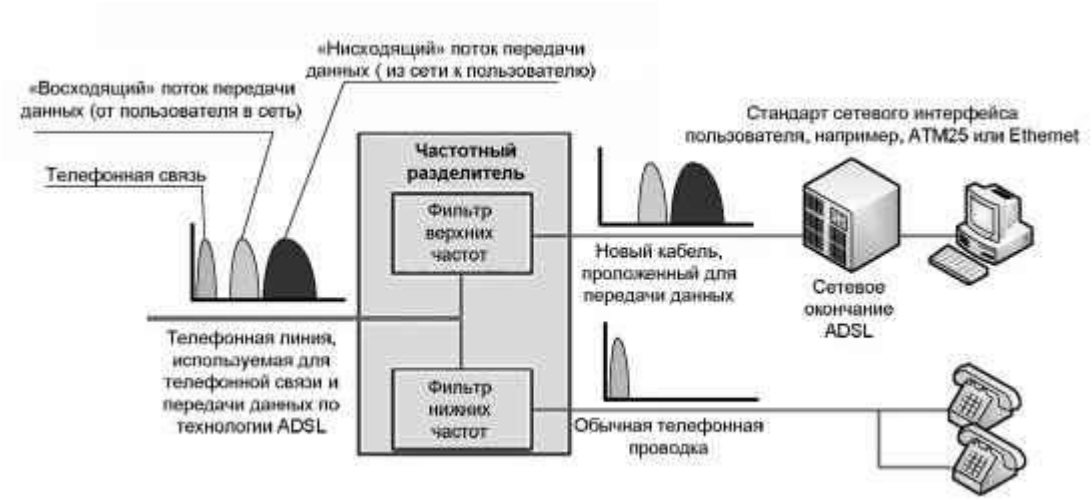


Рисунок 4.5 – Приклад ADSL із частотним ущільненням і сплітером

У рамках швидкісних каналів для передачі даних використовується стійка до вузькосмугових завад та шумів технологія DMT (Discrete Multi Tone), відповідно до якої вся вільна від телефонії смуга (від 26 кГц до 1,1 МГц для базової технології й до 2,2 МГц для ADSL2+) ділиться на елементарні канали шириною по 4,3125 кГц, і різні несучі одночасно переносять різні частини переданих даних. Величина максимально досяжної швидкості передачі/приймання даних при цьому залежить від довжини і якості телефонної лінії (рисунок 4.6).

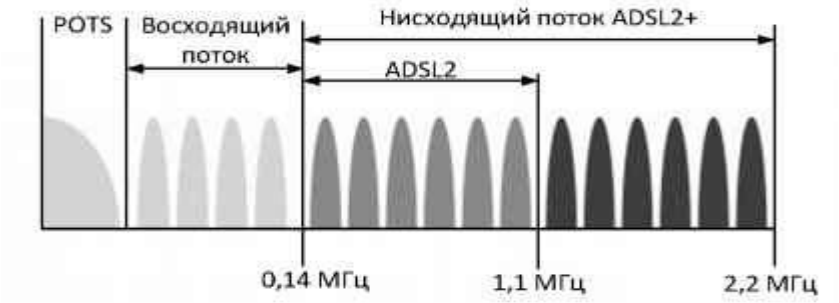


Рисунок 4.6 – Технології ADSL/ADSL2+: використання частотного діапазону лінії

На етапі перевірки якості лінії передавач, виходячи з рівня завад у частотному діапазоні ділянки, для кожного із цих каналів вибирає належну модуляційну схему.

На «чистих» каналах з малим рівнем шумів можуть бути використані методи модуляції з високим рівнем, наприклад QAM-64, на більш зашумлених ділянках – типу QPSK. Такий принцип регулювання швидкості обміну дозволяє найбільше точно погоджувати параметри модульованого сигналу з параметрами лінії, по якій він буде передаватися. При передачі даних інформація розподіляється між незалежними каналами пропорційно їх пропускної здатності, приймачу залишається виконати операцію демультиплексування й відновити вихідний інформаційний потік.

Технологія ***понадвисокошвидкісної цифрової абонентської лінії VDSL*** (Very High Bit-Rate Digital Subscriber Line) є найбільш «швидкою» асиметричною технологією xDSL. Вона забезпечує швидкість передачі даних «спадного» потоку в межах від 13 до 52 Мбіт/с, а швидкість передачі даних «висхідного» потоку в межах від 1,5 до 2,3 Мбіт/с, при чому по одній крученому парі телефонних проводів. У симетричному режимі підтримуються швидкості до 26 Мбіт/с.

Технологія VDSL є результатом природньої еволюції технології ADSL убік збільшення швидкості передачі даних і використання ще більш широкої смуги частот.

Стандарт HDSL (High Bit-Rate Digital Subscriber Line – високошвидкісна цифрова абонентська лінія) передбачає організацію симетричної лінії передачі даних, тобто швидкості передачі даних від користувача в мережу й з мережі до користувача рівні. Завдяки швидкості передачі (1,544 Мбіт/с по двом парам проводів і 2,048 Мбіт/с по трьом парам проводів) телекомунікаційні компанії використовують технологію HDSL у якості альтернативи лініям T1/E1 (лінії T1 використовуються в Північній Америці й забезпечують швидкість передачі даних 1,544 Мбіт/с, а лінії E1 використовуються в Європі й забезпечують швидкість передачі даних 2,048 Мбіт/с). Хоча відстань, на яку система HDSL передає дані (порядку 3,5-4,5 км) досить невелика, але є досить недорогим та ефективним рішенням. Для збільшення довжини лінії HDSL телефонні компанії встановлюють спеціальні повторювачі. Використання для організації лінії HDSL двох або трьох кручених пар телефонних проводів робить цю систему ідеальним варіантом для з'єднання АТС, серверів Інтернет, локальних мереж і т.п.

Технологія HDSL являє собою систему двосторонньої симетричної передачі даних, яка дозволяє передавати дані зі швидкістю 1,544 Мбіт/с або 2,048 Мбіт/с по декільком парам проводів мережі доступу. Рекомендовано два лінійні коди: амплітудно-імпульсна модуляція 2B1Q і амплітудно-фазова модуляція без несучої (CAP). Модуляція CAP використовується для передачі зі швидкістю 2,048 Мбіт/с, у той час як для модуляції 2B1Q визначено два різні цикли (рисунок 4.7).

Рисунок 4.7 – Еволюція систем передачі HDSL

Технологія ***однолінійної цифрової абонентської лінії SDSL*** (Single Line Digital Subscriber Line) також як і технологія HDSL, забезпечує симетричну передачу даних зі швидкостями, відповідними до швидкостей лінії T1/E1, але при цьому технологія SDSL має дві важливі відмінності:

– використовується тільки одна кручена пара проводів;
– максимальна відстань передачі обмежена 3 км.

Нова технологія ***HDSL2*** використовує 16-рівневу модуляцію PAM (Pulse Amplitude Modulation). Обраний спосіб модуляції PAM-16 забезпечує передачу трьох біт корисної інформації й додаткового біта (кодування для захисту від помилок) в одному символі. Сама по собі модуляція PAM не несе в собі нічого нового. Добре відома 2B1Q – це теж модуляція PAM, але чотирьохрівнева. Використання ґратчастих (Trellis) кодів, які за рахунок уведення надлишковості переданих даних дозволили знизити ймовірність помилок, дало виграш в 5 Дб.

Результуюча система одержала назву TC-PAM (Trellis coded PAM). При декодуванні в приймачі використовується досить ефективний алгоритм Вітербі.

Технологія ***надшвидкодіючих цифрових абонентських ліній SHDSL*** (англ. Single-pair High-speed DSL) забезпечує симетричну дуплексну передачу даних зі швидкостями від 192 кбіт/с до 2.3 Мбіт/с (із кроком в 8 кбіт/с) по одній парі проводів, відповідно від 384 кбіт/с до 4,6 Мбіт/с по двом парам.

При використанні методів кодування TC-PAM 128, стало можливим підвищити швидкість передачі до 15,2 Мбіт/с по одній парі й до 30,4 Мбіт/с по двом парам відповідно.

4.1.3. Реалізація систем доступу на основі ВОЛЗ

У цей час для надання користувачам широкосмугових послуг використовуються звичайно змішані мідно-оптичні мережі доступу. Існує кілька основних концепцій розгортання мережі доступу змішаного типу з використанням волоконно-оптичних ліній зв’язку:

– технологія HFC (Hybrid Fiber Coaxial) припускає доведення оптики до місця концентрації, при цьому далі розподільна абонентська мережа будується на основі коаксіальних кабелів. Дана архітектура не одержала широкого поширення й використовується звичайно лише операторами кабельного телебачення;
– концепція FTTx і її різні варіанти;
– технологія пасивних оптичних мереж (PON).

Група технологій FTTx (Fiber To The x – оптичне волокно до …) призначена для спільного використання з технологіями ADSL і VDSL і дозволяє більш ефективно використовувати пропускну здатність цих технологій завдяки скороченню довжини мідно-кабельних ліній зв’язку. Є кілька варіантів реалізації FTTx, з них можна виділити основні (рисунок 4.8):

– FTTH (Fiber To The Home) – доведення волокна до квартири;

– FTTB – (Fiber To The Building) – доведення волокна до будинку.

Варіанти, по суті, що дублюють FTTH і FTTB з невеликими змінами:

– FTTN (Fiber to the Node) – волокно до мережного вузла;

– FTTO (Fiber To The Office) – доведення волокна до офісу;

– FTTC (Fiber To The Curb) – доведення волокна до кабельної шафи;

– FTTcab (Fiber To The Cabinet) – аналог FTTC;

– FTTR (Fiber To The Remote) – доведення волокна до вилученого модуля, концентратора;

– FTTopt (Fiber To The Optimum) – доведення волокна до оптимального пункту;

– FTTP (Fiber To The Premises) – доведення волокна до місця присутності клієнта.

При цьому запланований набір послуг і необхідна для його надання смуга пропускання мають найбезпосередніший вплив на вибір технології FTTx. Тому чим вище швидкість доступу й чим більше набір надаваних абонентові послуг, тем ближче до абонентського термінала повинне підходити оптичне волокно, тобто потрібно використовувати технології FTTH. У випадку, коли пріоритетом є збереження вже наявної мережної інфраструктури й устаткування, оптимальним вибором буде FTTB.

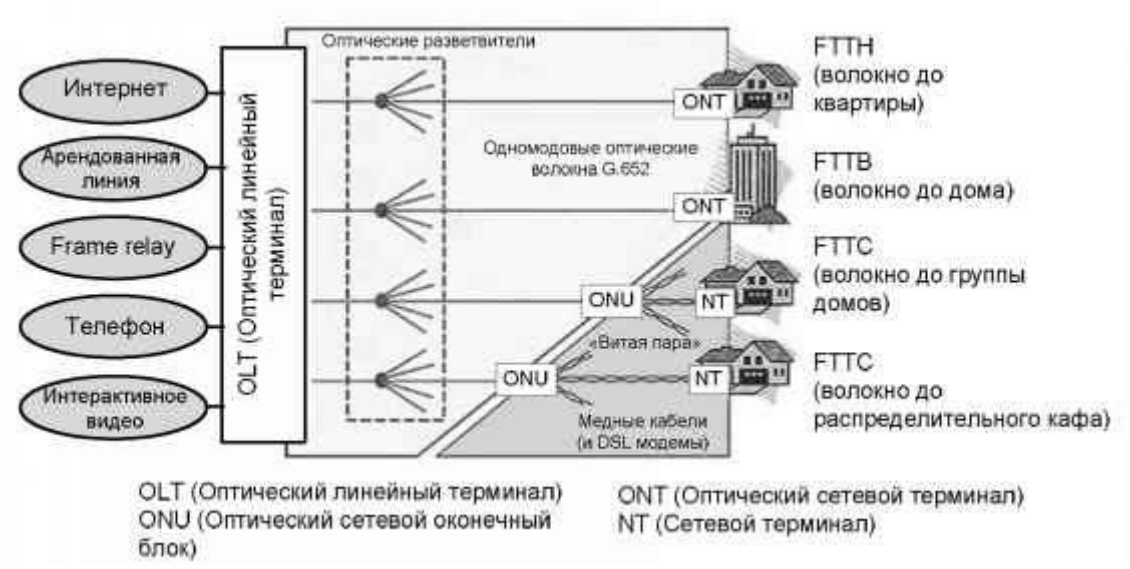


Рисунок 4.8 – Технології оптичного доступу FTTx

Підгрупа технологій ***пасивних оптичних мереж (PON)*** – це сімейство перспективних технологій широкосмугового мультисервісного множинного доступу по оптичному волокну. Сутність технології пасивних оптичних мереж, що випливає з її назви, полягає в тому, що її розподільна мережа будується без яких-небудь активних компонентів: розгалуження оптичного сигналу здійснюється за допомогою пасивних дільників оптичної потужності – сплітерів.

Технологія PON за економічними показниками більш пристосована до «килимового» покриття, ніж до точкових інсталяцій. За допомогою технології GPON стало можливим забезпечити доступ в Інтернет на

швидкості до 50 Гбіт/с і більш. Довжина оптоволоконного кабелю від мережного вузла до споживача може досягати 20 км або навіть 60 км.

Наслідком цієї переваги є зниження вартості системи доступу, зменшення обсягу необхідного мережного керування, висока дальність передачі й відсутність необхідності в наступній модернізації розподільної мережі.

Суть технології PON полягає в тому, що між приймально-передавальним модулем центрального вузла OLT (optical line terminal) і вилученими абонентськими вузлами ONT (optical network terminal) створюється повністю пасивна оптична мережа, що має топологію дерева (рисунок 4.9).

У проміжних вузлах дерева розміщуються пасивні оптичні розгалужувачі (сплітери, з коефіцієнтом розгалуження до 1:64 або навіть 1:128) – це компактні пристрої, що не вимагають живлення й обслуговування. Один приймально-передавальний модуль OLT дозволяє передавати інформацію безлічі абонентських пристроїв ONT.

Число ONT, підключених до одному OLT, може бути настільки більшим, наскільки дозволяє бюджет потужності й максимальна швидкість приймально-передавальної апаратури.

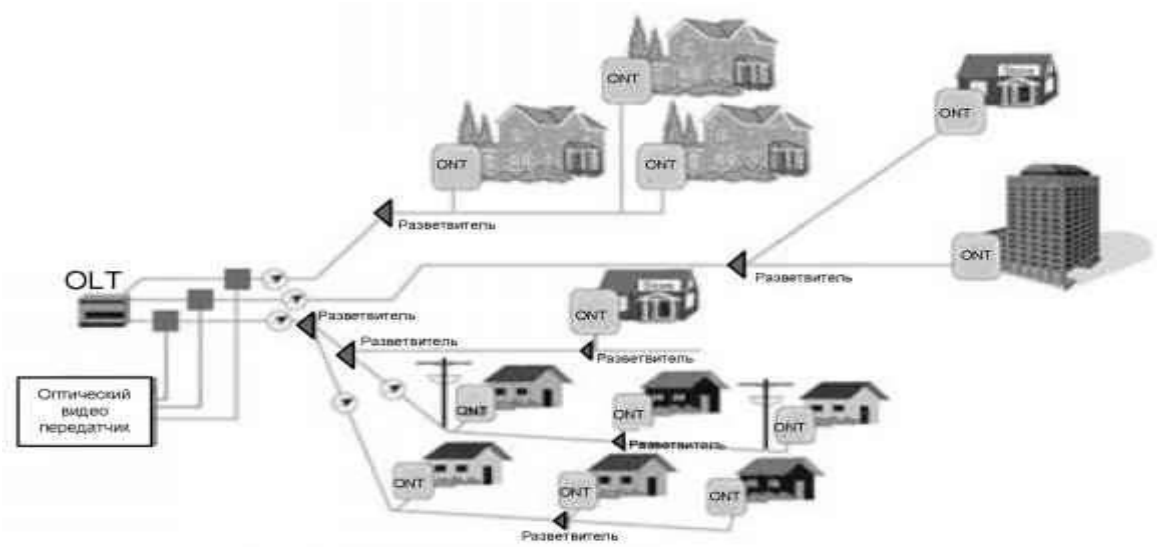


Рисунок 4.9 – Структура PON мережі

Для передачі прямого й зворотного каналу використовується одне оптичне волокно, смуга пропускання якого динамічно розподіляється між абонентами, або два волокна у випадку резервування. Спадний потік (downstream) від центрального вузла до абонентів іде на довжині хвилі 1490 нм і 1550 нм для відео.

Висхідні потоки (upstream) від абонентів ідуть на довжині хвилі 1310 нм із використанням протоколу множинного доступу з часовим поділом (TDMA). У деяких випадках використовується додаткова довжина хвилі спадного потоку (downstream), що дозволяє надавати традиційні аналогові й

цифрові телевізійні послуги користувачам без застосування телевізійних приставок з підтримкою IP.

Для побудови PON використовується топологія «точка-багатоточка» і сама мережа має деревоподібну структуру. Кожний волоконно-оптичний сегмент підключається до одному приймально-передавачу в центральному вузлі (на відміну від топології "точка-точка"), що також дає значну економію у вартості встаткування. Один волоконно-оптичний сегмент мережі PON охоплює до 32 абонентських вузлів у радіусі до 20 км для технологій EPON / BPON і до 128 абонентських вузлів у радіусі до 60 км для технології GPON (рисунок 4.10).

Кожний абонентський вузол розрахований на звичайний житловий будинок або офісний будинок і у свою чергу може охоплювати сотні абонентів. Усі абонентські вузли є термінальними, і відключення або вихід з ладу одного або декількох абонентських вузлів ніяк не впливає на роботу інших.

Архітектура FTTH на базі PON звичайно підтримує протокол Ethernet. Центральний вузол PON може мати мережні інтерфейси ATM, SDH (STM-1), Gigabit Ethernet для підключення до магістральних мереж. Абонентський вузол може надавати сервісні інтерфейси 10/100Base-TX, FXS (2, 4, 8 і 16 інтерфейсів для підключення аналогових телефонних абонентів), E1, цифрове відео, ATM (E3, DS3, STM-1) – рисунок 4.10.

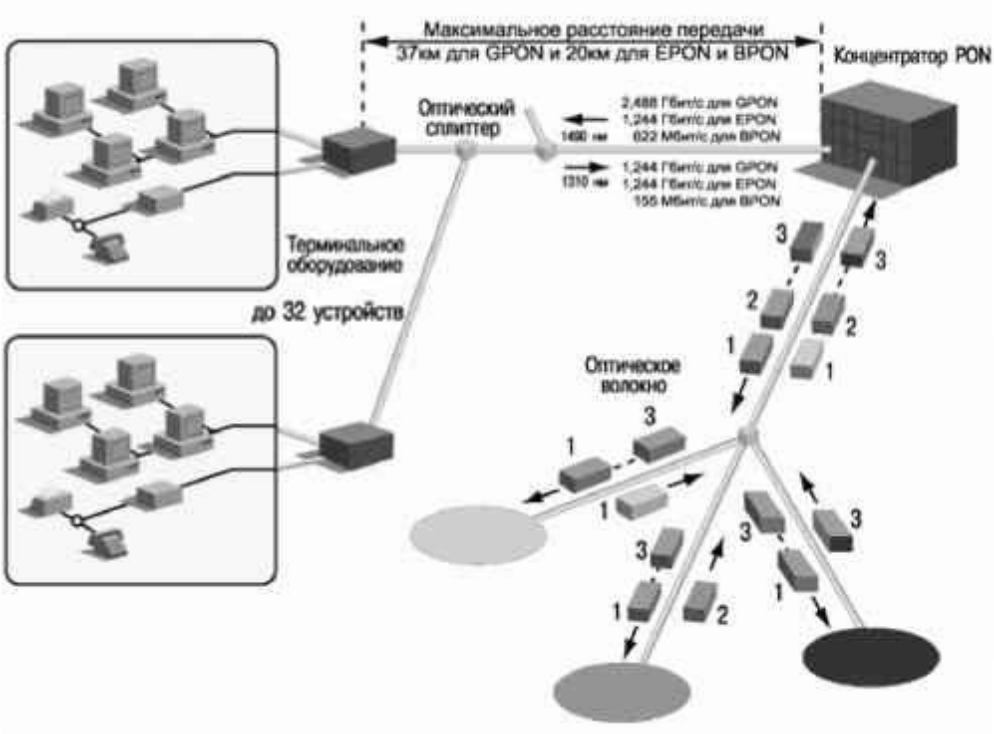


Рисунок 4.10 – Принцип часового поділу абонентів у технології PON

У сімействі мереж PON існує кілька різновидів, що відрізняються, у першу чергу, базовим протоколом передачі. Причому стандарти PON активно удосконалюються в напрямку збільшення швидкості передачі й дальності зв'язку.

Стандарт мережі APON був створений міжнародним консорціумом FSAN (Full Service Access Network) в 1995 році. До складу мережі APON входять:

– один мережний вузол OLT (Optical Line Terminal);
– до 32 абонентських терміналів ONU (Optical Network Unit);
– пасивні оптичні відгалужувачі (splitter).

У стандарті APON забезпечується швидкість передачі прямого й зворотного потоків по 155 Мбіт/с (симетричний режим) або 622 Мбіт/с у прямому потоці й 155 Мбіт/с у зворотному (асиметричний режим). Щоб уникнути накладення даних, що надходять від різних абонентів, OLT направляє на кожний ONU службові повідомлення з дозволом на відправлення даних.

Прямій і зворотний канали організують в одному оптичному волокні за рахунок хвильового ущільнення – передача до абонентів ведеться на довжині хвилі 1550 нм, а у зворотному напрямку – 1310 нм. Швидкість передачі інформації для індивідуального користувача становить 20 Мбіт/с, а максимальне видалення користувача від вузла доступу – 20 км. У цей час APON у своєму первісному виді практично не використовується.

Стандарт BPON з'явився в результаті еволюційного вдосконалювання технології PON. У BPON швидкість прямого й зворотного потоків доведена до 622 Мбіт/с у симетричному режимі або 1244 Мбіт/с і 622 Мбіт/с в асиметричному режимі. Передбачена можливість передачі трьох основних типів інформації (голос, відео, дані), причому для потоку відеоінформації виділена довжина хвилі 1550 нм. BPON дозволяє організовувати динамічний розподіл смуги між окремими абонентами. Після розробки більш високошвидкісної технології GPON, застосування BPON практично втратило сенс з економічних міркувань.

Стандарт EPON (Ethernet PON) з'явився в результаті використання технології Ethernet у локальних мережах і побудови на їхній основі оптичних мереж доступу. Такі мережі, в основному, розраховані на передачу даних зі швидкістю прямого й зворотного потоків 1 Гбіт/с на основі IP-протоколу для 16 (або 32) абонентів. Виходячи зі швидкості передачі, у статтях і літературних джерелах часто фігурує назва GEPON (Gigabit Ethernet PON), яке також відноситься до стандарту IEEE 802.3ah. Дальність передачі в таких системах досягає 20 км. Для прямого потоку використовується довжина хвилі 1490 нм, 1550 нм резервується для відео додатків. Зворотний потік передається на 1310 нм. Щоб уникнути конфліктів між сигналами зворотного потоку застосовується спеціальний протокол керування множиною вузлів (Multi-Point Control Protocol, MPCP).

Технологія GPON яка успадковує лінійку APON…BPON, але з більш високою швидкістю передачі – 1244 Мбіт/с, 2488 Мбіт/с (в асиметричному режимі) і 1244 Мбіт/с (у симетричному режимі) вважається найбільш вдалою для великих операторів, що будують розгалужені мережі із системами резервування. За основу GPON був прийнятий базовий протокол SDH (а точніше SDH на протоколі GFP, Generic Framing Procedure) з усіма

перевагами й недоліками, що притаманні йому. В GPON можливе підключення до 32 (або 64) абонентів на відстані до 20 км (з можливістю розширення до 60 км). GPON підтримує трафік ATM, IP, мови й відео (інкапсульовані в кадри GEM / GPON Encapsulated Method), а також модулі SDH. Мережа працює в синхронному режимі з постійною тривалістю кадру. Лінійний код NRZ зі скремблюванням забезпечують високу ефективність смуги пропускання. Єдиним серйозним недоліком GPON є висока вартість устаткування.

Технологія WDM PON є наступним ефективним кроком по збільшенню швидкості передачі побудованих систем PON за рахунок застосування систем оптичного ущільнення WDM. У рекомендації ITU-T G.983.2 описана можливість передачі сигналів на виділеній для кожного абонента довжині хвилі. У мережі передається загальний потік, а кожний абонентський термінал має оптичний фільтр для виділення своєї довжини хвилі. Технічно можливо забезпечити продуктивність системи зі швидкостями близько 4…10 Гбіт/с у кожному каналі. Після такої реконструкції провайдери одержать можливість вибудовувати пропускну здатність відповідно до вимог клієнта й успішно додавати або видаляти пристрої ONU без втручання в загальну інфрастуктуру, тобто в майбутньому впровадження систем WDM PON принесе реальні переваги операторам при незначних витратах.

Основні характеристики різновидів стандартів PON наведені в таблиці 4.3.

В GEPON, на відміну від GPON, відсутні специфічні функції підтримки TDM, синхронізації й захисних перемикань, що робить цю технологію самої економічної із усього сімейства. Особливо це стосується невеликих операторів, орієнтованих на IP-трафік, а згодом і IPTV. До того ж передбачається подальше развитее цього ряду – logepon (за аналогією з 10 Gb Ethernet). Тому через найкраще співвідношення ціна/якість при середньому розмірі мережі, у нашій країні варіант GEPON одержав найбільше поширення.

Технологія PON має ряд незаперечних переваг:

– невисока вартість побудови мережі;
– економія оптико-волоконного кабелю на ділянці;
– низькі витрати на експлуатацію й технічне обслуговування мережі;
– можливість поступового нарощування мережі;
– перспективність створення розподільної інфраструктури, що забезпечує в майбутньому розвиток будь-яких мультимедійних послуг із практично необмеженою смугою пропускання;
– висока надійність за рахунок використання пасивного встаткування.

Відзначимо типові проблемні питання, з якими зустрічаються провайдери, при розгортанні пасивної оптичної мережі PON.

Загальна смуга пропускання. Смуга пропускання в дереві оптоволоконних ліній мережі PON використовується як можна більшим числом абонентів. Хоча технологія GPON забезпечує загальну пропускну здатність спадного потоку 2,5 Гбіт/с, вона може не відповідати росту

майбутніх вимог абонентів у довгостроковій перспективі, оскільки потреби в пропускній здатності ростуть експоненціально.

Таблиця 4.3 – Порівняльна таблиця по характеристиках стандартів PON

Характеристики	**APON (BPON)**	**EPON (GEPON)**	**GPON**
Інститути стандартизації / альянси	ITU-T SGI 5 / FSAN	IEEE/ EFMA	ITU-T SGI5/FSAN
Дата прийняття стандарту	жовтень 1998	липень 2004	жовтень 2003
Стандарт	ITU-T G.981.x	IEEE 802.3ah	ITU-T G.984.X
Швидкість передачі,	155/155	1000/1000	1244/155, 622, 1244
прямій/зворотний потік,	622/155		2488/622, 1244, 2488
Мбіт/с	622/622		
Базовий протокол	ATM	Ethernet	SDH (GFP)
Лінійний код	NRZ	8B/10B	NRZ
Максимальний радіус мережі, км	20	20 (>30>)	20
Максимальне число	32	16	64 (1282)
абонентських вузлів			
на одне волокно			
Додатка	будь-які	IP, дані	будь-які
Корекція помилок FEC	передбачена	немає	необхідна
Довжини хвиль прямого/зворотного	1550/1310	1550/1310	1550/1310
потоків, нм	(1480/1310)	(1310/13103)	(1480/1310)
Динамічне	є	4 підтримка	є
розподіл смуги			
Ір-Фрагментація	є	немає	є
Захист даних	шифрування відкритими ключами	немає	шифрування відкритими ключами
Резервування	є	немає	є
Оцінка підтримки	висока	низька	висока
голосових додатку й QoS			
Динамічний діапазон, дБ:			
- клас А	5-20		5-20
- клас В	10-25		10-25
- клас І3	15-30		15-30
Інтерфейс РХ-10 (10 км)		5-20	
Інтерфейс РХ-20 (20 км)		10-24	

Примітки:

1. обговорюється в проекті; стандарт допускає нарощування мережі до 128 ONT;
2. допускається передача в прямому й зворотному напрямку на одній і тій же довжині хвилі;
3. здійснюється на більш високих рівнях.

Особливо, якщо деяку частину смуги пропускання необхідно резервувати для потокових послуг (наприклад, IPTV).

Шифрування. Оскільки PON – це технологія із загальним середовищем передачі, те необхідне шифрування всіх потоків даних. У технології GPON проводиться шифрування AES з 256-розрядними ключами тільки спадного потоку. Однак використання стандарту AES знижує продуктивність мережі, тому що при шифруванні необхідна передача істотного обсягу службової інформації разом з кожним пакетом.

Висока робоча швидкість кінцевих пристроїв. У зв'язку з використанням у пасивних оптичних мережах PON загального передавального середовища, кожне кінцевий пристрій (ONT або OLT) змушено працювати на єдиній максимальній швидкості передачі даних. Навіть якщо абонентові необхідна швидкість 25 Мбіт/с, кожна кінцева крапка оптичної мережі (ONT) у дереві PON повинна працювати на швидкості стандарту (2,5 Гбіт/с для GPON). Робота електронних і оптичних пристроїв зі швидкістю, в 100 раз перевищуючої необхідну швидкість передачі даних, підвищує ціну компонентів.

Необхідність великої потужності оптичного сигналу. При кожному розгалуженні в співвідношенні 1:2 енергетичний потенціал лінії зв'язку падає на 3,4 дБ. Отже, при розгалуженні в співвідношенні 1:64 енергетичний потенціал лінії зв'язку зменшується на 20,4 дБ (еквівалентно відношенню потужностей 110). У цьому випадку, усі оптичні передавачі повинні забезпечувати в 110 раз більшу потужність оптичного сигналу в порівнянні з архітектурою FTTH "точка-точка" при передачі на ту саме відстань.

Доступ до абонентських ліній. Відокремлення абонентських ліній (Local Loop Unbundling (LLU) – це метод, застосовуваний у мережах операторів телефонії для забезпечення доступу альтернативним операторам до абонентських мідних ліній зв'язку. Мережі PON поки не задовольняють вимогам LLU, оскільки є тільки одна оптоволоконна лінія для підключення групи абонентів, яка, отже, не може бути розділена на фізичному рівні, а тільки на логічному рівні. Ця особливість пасивної оптичної мережі на базі PON припускає масовий продаж послуг основного оператора без надання прямого абонентського доступу за допомогою відокремлення абонентських ліній (LLU).

Неоптимальне використання ресурсу мережі. Звичайно при розгортанні мережі FTTH виконується одночасне підключення оптоволоконних ліній зв'язку для всіх потенційних абонентів у даному районі. Абоненти можуть підписатися на сервіс FTTH тільки після розгортання всіх оптоволоконних ліній. При розгортанні послуг для

приватних абонентів провайдери рідко досягають 100% підписки. Звичайно цей показник близький до 30%, що означає, що частина структури PON простоює, а мережа в цілому використовується не оптимально.

Складність обслуговування, пошуку й усунення несправностей. Пасивні оптичні розгалужувачі не можуть передавати інформацію про несправності в центр керування мережею. Тому складно виявити несправність оптоволоконної лінії між розгалужувачем і точкою закінчення оптичної мережі (ONT) абонента.

Це значно ускладнює пошук і усунення несправностей у мережах PON і підвищує витрати на їхню експлуатацію. Так само при ушкодженні точки закінчення оптичної мережі (ONT), вона може передавати в дерево оптоволоконних ліній постійний світловий сигнал, що приводить до порушення зв'язку для всіх абонентів цієї мережі, причому знайти ушкоджений пристрій дуже важко.

4.2. Технології транспортних телекомунікаційних мереж

4.2.1. Транспортні мережі METRO

Транспортні мережі територіальних сегментів MAN і WAN (масштабу міста, великого регіону) як мережі загального користування (публічні мереж) отримали назву ***"транспортні мережі МЕТРО"*** (з англійської Metropolitan – місто, мегаполіс). Їх завданням є перерозподіл транзитного трафіку, який створюють не лише окремі користувачі, а й сегменти LAN. Усі вони висувають різні вимоги до транспортування інформації з кінця в кінець. Таким чином, транспортні мережі МЕТРО необхідно будувати, враховуючи можливості надання так званого диференційованого сервісу в точках входу-виходу (вузлах доступу) транспортної мережі, що забезпечує налаштування гнучких і прозорих з'єднань, які передають пакетовані дані (кадри, комірки) канального рівня поверх фізичного рівня.

На відміну від сегментів LAN, транспортні мережі МЕТРО перетворюються на дворівневу телекомунікаційну інфраструктуру, яка містить технології фізичного й канального рівнів. Таку архітектуру називають **платформою надання сервісів** (Service Provisioning Platform, **SPP).** На рисунку 4.11 наведено архітектуру такої мережі.

Рисунок 4.11 – Архітектура транспортної мережі МЕТРО

Якщо в сегментах LAN фізичний рівень базується в основному на використанні ліній, обмеження на фізичну довжину яких передбачено стандартами структурованих кабельних систем (СКС), то в територіальних транспортних мережах довжина ліній зв'язку є досить великою, отже, і вартість, відповідно, дуже високою. У зв'язку з цим гостро постає питання ефективності використання смуги пропускання таких ліній. Крім того, в публічних мережах необхідно забезпечувати можливість задоволення запитів різних користувачів та надання різноманітних сервісів (організацію різних режимів перенесення інформації, смуги пропускання каналів).

Таким чином, фізичний рівень транспортної мережі METPO перетворюється у відносно самостійну мережу, в якій застосовано специфічні для неї технології фізичного рівня, що надають **первинні сервіси** (Background Services) канального рівня у вигляді *каналів точкових з'єднань з заданою смугою пропускання.*

На канальному рівні реалізується комутована топологія з використанням первинного сервісу для організації зв'язків між вузловими пунктами, в яких налаштовується комунікаційне обладнання відповідної *базової телекомунікаційної технології канального рівня*, *яке надає* **сервіси *базових мережних технологій*** (Network Based Services), тобто технологій канального рівня. Їх називають ***"базовими сервісними мережами"***.

У територіальних (MAN, WAN) телекомунікаційних мережах використання спільного комунікаційного середовища здійснюється шляхом його поділу на множини незалежних каналів двоточкового з'єднання пари пунктів (вузлів доступу). Спільне середовище передавання в даному випадку, як відомо, можна розподіляти за частотою (FDM), за часом (TDM), за довжиною хвилі (WDM). Як комунікаційне обладнання вузлів доступу застосовують різні мультиплексори.

Мультиплексори забезпечують спільне використання фізичної лінії, під'єднаної до єдиного виходу мультиплексора, декількома інформаційними потоками, які надходять на його входи. При цьому середовище передавання вихідної лінії поділяється на канали, кількість яких дорівнює кількості входів. Поділяти можна за частотою або за часом зайняття. Розрізняють мультиплексори сегментів доступу й транспортних сегментів. При цьому беруться до уваги також технологічні особливості фізичного рівня передавання сигналів у широкосмугових середовищах.

Виокремлюють три покоління транспортних технологій фізичного рівня METRO:

- плезіохрона цифрова ієрархія (PDH);
- синхронна цифрова ієрархія (SDH);
- щільне хвильове мультиплексування (DWDM).

Перші дві технології підтримують ієрархії швидкостей, тому, організувавши інформаційний обмін між під'єднаними повільними сегментами, можна вибрати будь-яку відповідну швидкість передавання цифрових потоків.

Технологія DWDM стала більш пізнім досягненням у сфері створення високошвидкісних каналів. Вони не є цифровими, тому що надають для передавання інформації відокремлену (виділену) хвилю.

4.2.2. Технологія SDH

Прагнення подолати недоліки PDH-технології призвело до розробки у 1984-1986-х роках у США ієрархії синхронної оптичної мережі (Synchronous Optical Network, **SONET),** а в Європі – **синхронної цифрової ієрархії** (Synchronous Digital Hierarchy, **SDH).** Обидві ієрархії орієнтовані на використання ВОЛЗ.

Цифрові мережі, які застосовують синхронні телекомунікаційні технології, мають загальномережну синхронізацію від центрального опорного джерела (центрального таймера), точність якого не гірша від 10^{-9}.

Необхідність вирівнювати швидкості вихідних потоків у даному випадку майже відсутня, а це забезпечує можливість формувати фрейми фіксованого формату, використовуючи *байт-інтерлівінг* на всіх рівнях мультиплексування. Фіксований формат дає змогу чітко позиціонувати в структурі фрейму розташування полів, відповідних каналам зі швидкістю 64 кбіт/с, 2 Мбіт/с та ін.

Основним форматом вихідного синхронного потоку є так званий **синхронний транспортний модуль STM-1,** який забезпечує швидкість передавання 155,52 Мбіт/с та дає змогу інкапсулювати (вставляти) в нього всі фрейми європейської PDH ієрархії (E1, E2, E3 та E4).

У структури STM наявними є спеціальні покажчики початку будь-якого інкапсульованого фрагменту. Ці покажчики розміщують у поле заголовку фрейму STM. Використання покажчиків значно спрощує процедуру відокремлення потоків, різних швидкостей із загального цифрового потоку та дає змогу гнучко компонувати внутрішній формат STM.

Побудова швидкостей ієрархії SDH ґрунтується також на використанні коефіцієнтів мультиплексування. У SDH ці коефіцієнти набувають постійного значення, яке дорівнює 4, та фігурують у назві транспортного модуля у вигляді співмножника: STM-1 (155,52 Мбіт/с); STM-4 (622 Мбіт/с); STM-16 (2,5 Гбіт/с); STM-64 (10 Гбіт/с) та ін.

Таким чином, розробникам технології SDH вдалося не тільки забезпечити нарощування швидкостей передавання, але й урахувати стандарти наявної технології PDH, використовуючи вже відому на той час технологію інкапсуляції даних (технологію інкапсуляції застосовано в протоколі TCP/IP мережі Internet для транспортування IP-пакетів через мережі з різними архітектурами). У SDH – технології принцип інкапсуляції розвинуто у ***технологію віртуальних контейнерів***.

Контейнерами називаються фрейми стандартних розмірів із приєднаними до них заголовками. У полях заголовка міститься інформація, необхідна для маршрутизації, та покажчики початку розміщення потоків

різних швидкостей, які надходять з каналів доступу. Ці потоки називаються ***трибами***.

Цифрові потоки каналів доступу зі швидкостями передавання, відповідними стандартному ряду PDH, називають ***трибами PDH***, а потоки каналів доступу зі швидкостями передавання, відповідними стандартному ряду SDH – ***трибами SDH***.

Кожен триб (трибний потік) інкапсулюється у відповідний йому за розміром контейнер, забезпечений своїм заголовком. Так, наприклад, сформований після інкапсуляції триба 140 Мбіт/с контейнер визначив розмір поля корисного навантаження синхронного транспортного модуля STM-1 в 2349 байт, а долучення до нього полів заголовків – розмір самого STM-1: 2430 байт або 2430 × 8 = 19440 біт , що з частотою повторення 8000 Гц визначає швидкість породжувального члена ряду для ієрархії SDH: 19440 × 8000 = 155,52 Мбіт/с.

Цикл передачі STM-1 представляють таблицею розміром в 270 стовпців і 9 рядків, отже, він містить 270 × 9 = 2430 байт. З них 9×9 = 81 байт відведено під поле службових сигналів. Це поле складає всього лише 3,33% від загального поля циклу передачі, проте цього достатньо, щоб розмістити в ньому необхідні керуючі і контрольні сигнали і виділити частину байтів для утворення різних каналів службового зв'язку.

Для забезпечення наступності та підтримки рекомендацій ITU-T по плезіохронна ЦСП, термінальні мультиплексори (ТМ) та мультиплексори виділення / вставки (ADM) систем передачі SDH розраховані на оперування тільки тими цифровими потоками, швидкості передачі яких відповідають об'єднаному (американському і європейському) стандартним ряду плезіохронної ієрархії, а саме: 1,554; 2,048; 6,312; 8,448; 34,368; 44,736; 139,264 Мбіт / с, тобто цей ряд містить 7 членів. З цих вхідних (переданих) сигналів плезіохронних ЦСП в ТМ технології SDH формується цифровий потік зі швидкістю передачі 155,52 Мбіт / с, який називається первинним цифровим потоком (у системах передачі SDH).

Подальше формування стандартних швидкостей передачі в технології SDH здійснюється за геометричною прогресією виду 1, 4, 16, 64, 256. Слідуючи цьому ряду коефіцієнтів, який дозволяє розробникам обладнання систем передачі SDH мати постійний коефіцієнт мультиплексування, рівний чотирьом, в даний час проводяться системи передачі SDH з швидкостями передачі 155,52; 622,08; 2488,32; 9953,28; 39813,12 Мбіт/с відповідно до Рекомендацій ITU-T G.707/Y.1332 і G.709.

Елементи структури циклів передачі

Для побудови структури циклів передачі сигналів першого рівня ієрархії синхронних ЦСП використовуються складові елементи, або інформаційні структури, що формуються тільки в системах передачі SDH. До цих елементів відносяться:

- контейнер С;
- віртуальний контейнер VC;
- субблок TU;

– груповий субблок TUG;
– адміністративний блок AU;
– груповий адміністративний блок AUG;
– синхронний транспортний модуль STM-1.

Контейнери CN – це контейнери рівня N. Кожен контейнер являє собою фрагмент цифрового групового сигналу (ЦГС) заданої структури.

Віртуальні контейнери VC-N – це однойменні контейнери відповідного рівня. Кожен VC являє собою фрагмент ЦГС заданої структури, яка утворюється об'єднанням сигналів контейнера і трактового заголовка, тобто умовно визначається формулою VC = C + POH. Так як контейнер містить корисну навантаження PL (PayLoad), то в деяких джерелах формула для структури VC умовно представляється у вигляді: VC = PL + POH.

Субблоки TU, відповідно до VC, що входять до їх складу, позначають TU-1, TU-2 і TU-3. Вони, як і VC, діляться на два підрівні, а саме: TU-1 розбивається на TU-11 і TU-12; TU-2 - на TU-21 і TU-22; TU-3 - на TU-31 і TU -32.

Всі субблоки забезпечують узгодження при мультиплексуванні декількох сигналів мережного шару трактів нижчого порядку з мережним шаром тракту вищого порядку. Кожен субблок являє собою фрагмент ЦГС заданої структури, яка формується шляхом з'єднання сигналів VC і покажчика субблока (TU-покажчика), тобто визначається наступним чином: TU = VC + TU-вказівник. Покажчик субблока показує, на скільки потрібно відступити початку циклу передачі сигналів навантаження (VC-1 або VC-2) від початку циклу передачі сигналів VC вищого порядку (VC-3 або VC-4).

Груповий субблок TUG являє собою один або кілька субблоков і є фрагментом ЦГС заданої структури, який займає певні фіксовані позиції в навантаженні VC вищого порядку. Розрізняють два варіанти групових субблоков: TUG-2 і TUG-3.

Адміністративний блок AU призначений для узгодження сигналів мережного шару трактів вищого порядку з мережним шаром мультиплексних секцій. Кожен AU (AU-3 або AU-4) являє собою фрагмент ЦГС заданої структури, яка формується шляхом об'єднання сигналів корисного навантаження (VC-3 або VC-4) і AU-покажчика (AU-pointer), тобто визначається виразом: AU = VC + AU-вказівник. Початок циклу передачі сигналів корисного навантаження може переміщатися щодо початку циклу передачі мультиплексной секції, тому AU-вказівник визначає (вказує) адреса початку циклу передачі сигналів корисного навантаження, місце якого фіксоване.

Адміністративний блок AU-3 розбивається на два підрівні AU-31 і AU-32, корисне навантаження яких формується з VC-31 і VC-32 відповідно.

Адміністративний блок AU-4 не розбивається на підрівні.

Груповий адміністративний блок AUG являє собою один або кілька AU і є фрагментом ЦГС заданої структури, який займає певні фіксовані позиції в навантаженні STM-1. Блок AUG формується з AU-3 і AU-4 з різними коефіцієнтами мультиплексування, зокрема, як 1×AU-4, або

4×AU-31, або 3×AU-32. Далі AUG використовується, як корисне навантаження сигналу STM-1.

Синхронний транспортний модуль STM-1 являє собою повний цикл передачі ЦГС заданої структури в системі передачі SDH першого рівня. Крім корисного навантаження STM-1 містить службові сигнали, які також називають заголовками. Оскільки STM-1 використовується в мережному шарі секцій, то його заголовок називається секційним – SOH. Цикл передачі сигналу утворюється побайтное об'єднанням сигналів корисного навантаження AUG і сигналів SOH: STM-1 = AUG + SOH. Структура SOH підрозділяється на заголовок мультиплексной секції MSOH і заголовок регенераційної секції RSOH.

У результаті використання описаних вище елементів і їх варіантів, утворених наявністю підрівнів, можна зобразити схему побудови циклу передачі сигналу STM-1 (рисунок 4.12), запропоновану в першому варіанті Рекомендації ITU-T G.109 (1988).

Згідно з основною схемою мультиплексування для ієрархії SDH, модулі STM-1 далі можуть мультиплексуватися з коефіцієнтом n, кратним 4 (як уже зазначалося вище), а потім передаватися лінією зв'язку.

Основним функціональним обладнанням систем передачі SDH є синхронні мультиплексори SM (Synchronous Multiplexers). Вони виконують такі основні функції:

1) аналого-цифрове перетворення переданих сигналів і мультиплексування отриманих в результаті цього перетворення цифрових сигналів в цифрові потоки;

2) виділення / вставку переданих цифрових потоків в заданих пунктах мережі та їх оперативне переключення;

3) передачу цифрових сигналів по волоконно-оптичних і радіорелейних (супутникових) синхронних лінійних трактах. Крім того, SM задіяні у функціях контролю, управління, обслуговування та конфігурування мережі.

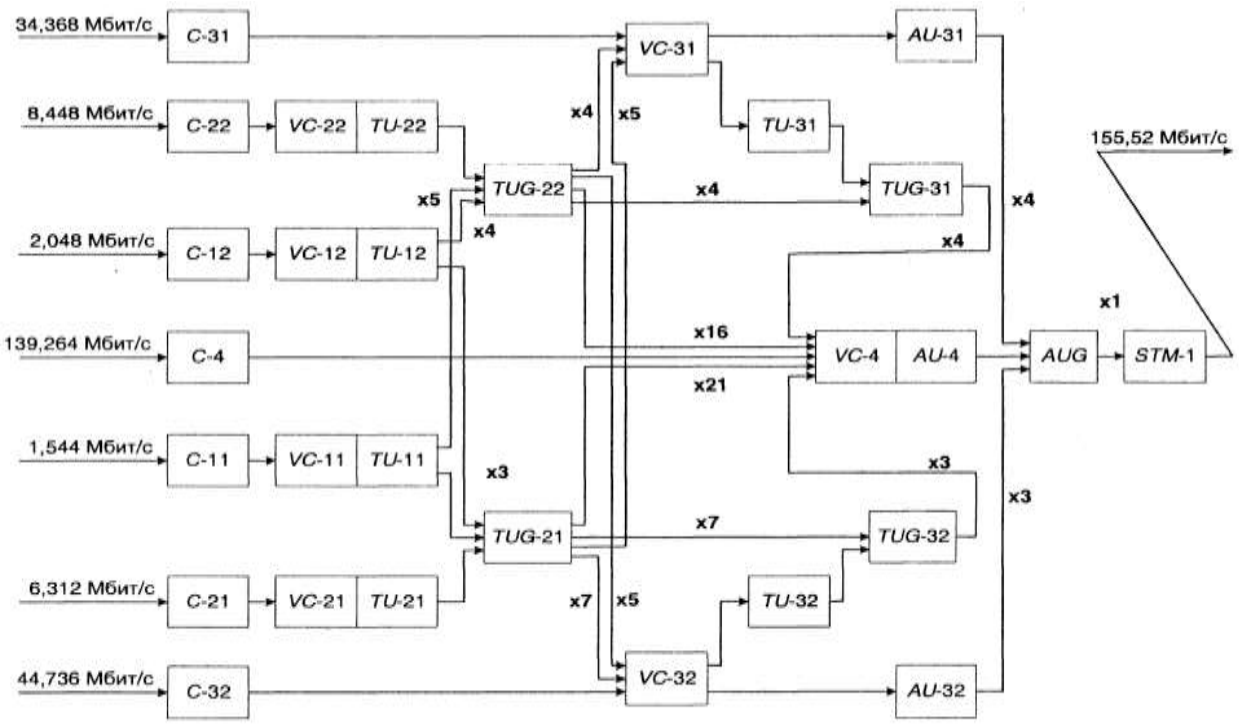


Рисунок 4.12 – Схема побудови циклу передачі сигналу STM-1

Розрізняють три основних типи SM:

– термінальні (кінцеві) мультиплексори TM (Terminal Multiplexers);

– синхронні лінійні мультиплексори SLM (Synchronous Line Multiplexers);

– мультиплексори виділення / вставки DIM (Drop / Insert Multiplexers), або мультиплексори введення / виведення ADM (Add / Drop Multiplexers).

Термінальні мультиплексори – це обладнання, або апаратура пунктів доступу систем передачі SDH, яка забезпечує зв'язок між двома пунктами, тобто в структурі мережі SDH "точка-точка". Ця апаратура призначена для гнучкого перетворення аналогових і мультиплексування цифрових переданих сигналів споживачів в цикли передачі первинних цифрових потоків, а також подальшого формування з сигналів цих потоків циклу передачі синхронного транспортного модуля рівня STM-1 (155,52 Мбіт/с). На прийомі термінальні демультіплексори розділяють прийнятий сигнал STM-1 на первинні цифрові потоки і на більш дрібні цифрові потоки зі швидкостями передачі 64, 144 і $n \times 64$ кбіт / с, де $n = 2, 3, ..., 30$.

Синхронні лінійні мультиплексори – це мультиплексори вищих рівнів ієрархії систем передачі SDH: SLM-4, SLM-16, SLM-64 і SLM-256, які є кінцевою апаратурою оптичного цифрового лінійного тракту. Лінійні мультиплексори SLM-4, SLM-16, SLM-64 і SLM-256 призначені для об'єднання 4, 16, 64 і 256 синхронних цифрових потоків рівня STM-1 в синхронні потоки транспортних модулів STM-4, STM-16, STM-64 , STM-256 відповідно.

Електричні сигнали результуючих потоків на виходах мультиплексорів SLM-4, SLM-16, SLM-64 і SLM-256 перетворюються в оптичні ЦЛС, які

передаються по ООВ оптичних лінійних кабелів зі швидкостями передачі 622,08 Мбіт / с; 2448,32 Мбіт / с (2,5 Гбіт / с); 9953,28 Мбіт / с (10 Гбіт / с) і 39813,12 Мбіт / с (40 Гбіт / с) відповідно.

Мультиплексори виділення / вставки, або введення / виведення – це апаратура проміжних пунктів систем передачі SDH, що забезпечує в цих пунктах виділення і вставку цифрових потоків для місцевого використання, транзит цифрових потоків, а також можливість розгалуження даного цифрового лінійного тракту (ЦЛТ) на лінійні тракти меншою пропускної здатності. Синхронні DIM мають ті ж рівні ієрархії, що і системи передачі SDH. Практично розроблені і застосовуються на мережах такі мультиплексори: DIM-1, DIM-4 і DIM-16.

Для подолання обмежень у відстані між мультиплексорами введення-виведення використовують регенератори сигналів (рисунок 4.13).

Рисунок 4.13 – Транспортний ланцюг

Синхронні мережі мають ряд переваг над плезіохроними, основні з яких:

– *спрощення мережі* – в синхронній мережі один мультиплексор введення/виведення дає змогу безпосередньо долучити або вилучити, наприклад, потік E1 (2 Мбіт/с) з фрейму STM-1 (155 Мбіт/с), замінюючи тим самим «гірлянду» мультиплексорів PDH;

– *прозорість для передавання будь-якого трафіку* досягається застосуванням віртуальних контейнерів для передавання трафіку, сформованого використанням інших технологій (Frame Relay, ISDN, ATM);

– *універсальність застосування* проявляється у тому, що технологія може бути використана як для створення окремих високошвидкісних магістралей METRO (мереж загального користування), так і для корпоративних мереж кільцевої топології.

З появою SDH-технології телекомунікаційні мережі доповнилися поняттями «пакування даних», «транспортування даних», у результаті виник термін ***«транспортна мережа»***.

4.2.3. Хвильове мультиплексування (WDM)

Волоконно-оптичний кабель (ВОК) характеризується будівельної довжиною (довжиною безперервної ділянки на одному барабані), вона змінюється залежно від типу кабелю в межах від 2 до 10 км. Окремі кабелі

з’єднують зварюванням оптичних волокон. На кожній ділянці ВОК кінці захищено спеціальною герметичною прохідний муфтою.

Усі оптичні волокна поділяють на дві групи: **багатомодові** (Multi Mode Fiber, **MMF)** та **одномодові** (Single Mode Fiber, **SMF).** Модами називаються різні типи світлових променів.

Використання багатомодового волокна обмежено локальними мережами з типовими довжинами сегментів до 2 км.

Одномодове волокно має більш високу пропускну здатність, його використовують тільки на протяжних магістралях. Однак воно вимагає застосування дорогих лазерних передавачів.

Передавання інформації волоконно-оптичними лініями зв’язку має багато переваг, у порівнянні з передаванням по мідному кабелю. Стрімке впровадження в транспортні мережі оптичних ліній стало результатом визнання цих переваг, зумовлених специфікою поширення сигналу в оптичному волокні:

– *широку смугу пропускання* уможливлено надзвичайно високими параметрами частоти-носія – 10^{14} Гц, що дає змогу передавати одним оптичним волокном інформацію в кілька терабіт за секунду. Широка смуга пропускання є однією з найважливіших переваг оптичного волокна, в порівнянні з мідним або будь-яким іншим середовищем передавання інформації;

– *висока завадозахищеність* – несприйнятливість до електромагнітних завад, які можуть виникати від мідних кабельних систем та електричного обладнання, які створюють електромагнітне випромінювання, оскільки волокно виготовляється з діелектричного матеріалу. У багатоволоконному кабелі також не можливий перехресний вплив електромагнітного випромінювання, властивий багатопарним мідним кабелям;

– *мале загасання світлового сигналу* у волокні, від 0,2 до 0,3 дБ на довжині хвилі 1,55 мкм у розрахунку на 1 км, а також невелика дисперсія, що дає змогу будувати ділянки ліній без ретрансляції протяжністю до 100 км і більше;

– *висока захищеність від несанкціонованого доступу* завдяки тому, що ВОК практично не має випромінювання в радіодіапазоні, а тому важко «прослухати» інформацію, що передається, не порушуючи прийому/передавання;

– *гальванічна розв’язка елементів мережі* обумовлена ізолювальною властивістю волокна. Це унеможливлює виникнення електричних «земельних» петель (наприклад, коли два мережних пристрої неізольованої мережі, пов’язані мідним кабелем, мають заземлення в різних точках будівлі, виникає різниця потенціалів, здатна пошкодити мережне обладнання);

– *пожежобезпечність* особливо важливою є для обслуговування технологічних процесів підвищеного ризику (на хімічних, нафтопереробних підприємствах);

– *мала вага й обсяг* у порівнянні з мідним кабелем у розрахунку на одну й ту ж пропускну здатність.

Поява технології багаточастотних напівпровідникових лазерів, здатних випромінювати різні довжини хвиль, дозволяє створити системи з оптичним мультиплексуванням, що різко підвищує сумарну швидкість передачі інформації в одному волокні. Такі системи отримали назву волоконно-оптичних систем із спектральним розділенням по довжині хвилі – ВОСП СР (Wavelength Division Multiplexing, WDM).

С точки зору збільшення пропускної спроможності переваги систем WDM очевидні. При цьому найбільш доцільним є використання комбінованого методу ущільнення, при якому на першому етапі застосовується часове розділення каналів (ЧасРК), які передаються в одному інформаційному потоці, а на другому – розділення окремих потоків (групових цифрових сигналів) по довжині хвилі.

Структурна схема WDM-системи має вигляд, представлений на рисунку 4.14, де показаний один напрям передачі. Передавальна частина системи отримує N вхідних потоків даних (групових цифрових послідовностей). Як приклад, на першому каналі показаний SDH-мультиплексор (SMUX), на N-ом каналі – АТМ-мультиплексор. Ці потоки обробляються відповідними інтерфейсними блоками $Інт_i$ і перетворюються в оптичний вигляд в оптичних модуляторах M_i з різними довжинами хвиль несучих λ_i. Модульовані оптичні несучі мультіплексуються (об'єднуються) за допомогою WDM-мультиплексора (MUX) в сумарний потік, який після посилення оптичним підсилювачем (ОП) подається в оптичну лінію зв'язку. У тракті передачі через певні відстані також встановлюються лінійні оптичні підсилювачі (ОП).

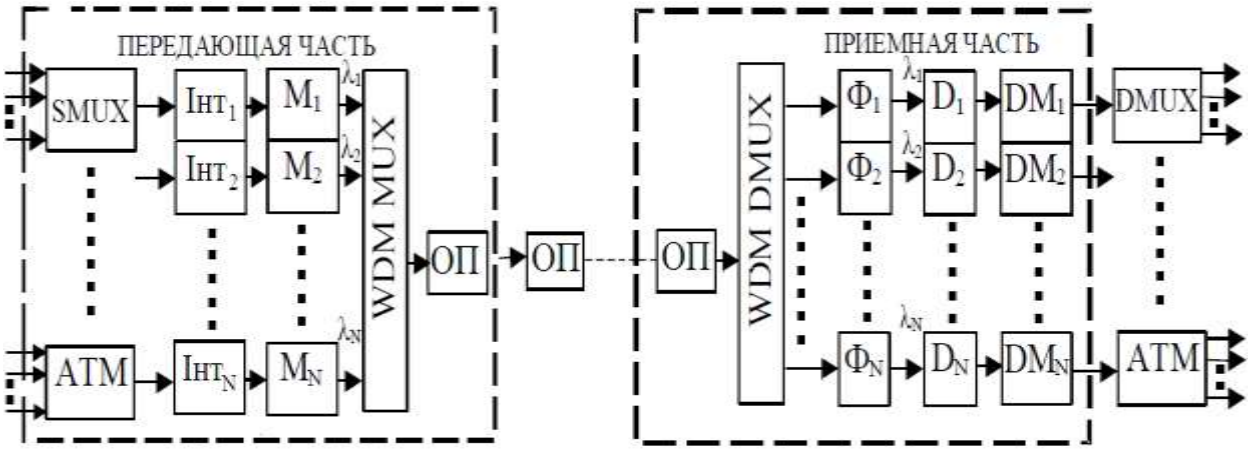


Рисунок 4.14 Структура одного напряму системи WDM

Приймальна частина системи, підсиливши прийнятий потік попереднім оптичним підсилювачем (ОП) демультиплексує його, тобто розділяє на компоненти з різними несучими, які детектуються за допомогою детекторів D_i. В результаті відновлюються початкові кодовані цифрові послідовності, що подаються потім на вхід демультиплексорів відповідних технологій.

Стандарти WDM-систем

Первинне хвильове мультиплексування було направлено на об'єднання двох несучих хвиль (1310 і 1550 нм) в одному оптоволокні, що дозволяло подвоїти ємкість системи і в даний час застосовується в багатьох стандартних системах SDH. Спектр таких WDM-систем не був суцільним, а складався з двох ізольованих смуг, які рознесені по довжині хвилі на 240 нм.

Наступним кроком в розвитку систем WDM стала технологія, що отримала назву розріджених систем WDM, або CWDM, в яких застосовується крок між несучими 20 нм (≈2,5 ТГц). Ці системи використовують широкий діапазон хвиль, що перекриває в суміжних вікнах прозорості (3 і 4) смугу порядка 82 нм (1528…1610 нм). Але відомі також більш широкосмугові системи CWDM, які використовують оптичні волокна компаній Corning або OFS (у яких усунений пік поглинання "ОН" в області 1383 нм).

Для забезпечення сумісності устаткування різних виробників систем WDM, MCE був стандартизований (G.692) номінальний ряд несучих і сформований так званий "частотний план". Він грає для систем WDM ту ж роль, що і цифрові ієрархії PDH і SDH для однойменних систем, тобто дає виробникам орієнтир на майбутнє і дозволяє позиціонувати вже існуючі системи WDM.

В основу стандарту був покладений частотний план з рівномірним розташуванням несучих частот каналів і мінімальним кроком несучих в 100 ГГц. Стандарт передбачав використання діапазону найбільш пристосованого для використання EDFA підсилювачів (1530…1570 нм). Зазначений крок дозволяв в цьому діапазоні (190,9…195,9 ТГц) розмістити максимально 51 канал (таблиця 4.4).

Таблиця 4.4 – Канали систем CWDM

Номер каналу	Частота, ТГц	Довжина хвилі, нм
1	195,9	1530
2	195,8	1531,12
3	195,7	1531,9
---	---	---
49	191,1	1568,77
50	191	1569,59
51	190,9	1570,42

Потім стандарт був допрацьований і крок був зменшений до 50 ГГц, що дозволяло розмістити більшу кількість каналів. Щоб отримати більші кроки у новому стандарті пропонувалося не використовувати певні довжини хвиль. Наприклад, для кроку 100 ГГц отримаємо окремий випадок, де фігурує кожна друга несуча. Аналогічно можна отримати окремі випадки для кроку: 200

ГГц (крок по ≈1,6 нм), 400 ГГц (≈3,2 нм), 600 ГГц (≈4,8 нм) і 1,0 ТГц (≈8,0 нм).

Подальше зменшення стандартного кроку несучих до 25 ГГц (161 несуча з кроком ≈0,2 нм) і навіть до 12,5 ГГц (321 несуча з кроком ≈0,1 нм) було запропоновано розробниками у вигляді нових стандартів G.694.1 та G.694.2 з новою редакцією частотного плану, який фактично узаконив вже оголошені низькою провідних виробників системи з 160…320 каналами. Таким чином, сучасна схема класифікації WDM-систем вдає із себе наступний перелік:

– розріджені WDM – CDWM-системи з кроком по довжині хвилі 20 нм;

– звичайні WDM – WDM-системи з кроком несучих по частоті більше 200 ГГц(≈1,6 нм), що дозволяють об’єднувати не більше 16 каналів;

– щільні WDM – DWDM-системи з кроком несучих по частоті від 100(≈0,8 нм) до 50 ГГц(≈0,4 нм);

– високо-щільні WDM – HDWDM-системи з кроком по частоті менше 50 (25(≈0,2 нм) і 12,5(≈0,1 нм)) ГГц.

На цьому інтенсивний шлях розвитку систем WDM, заснований на зменшенні кроку що несучих, можна, мабуть, вважати завершеним.

Розширення числа каналів систем WDM можна також досягти екстенсивним шляхом, заснованим на розширенні використовуємого оптичного діапазону Наприклад, зазначені стандарти передбачають розширені границі оптичних діапазонів, що можуть використовуватися для функціонування WDM-систем (таблиця 4.5). Поки важко уявити, що весь цей простір буде заповнений несучими, оскільки бавить при кроці 100 ГГц це 610 окремих оптичних каналів. Якщо в кожному з них передавати принаймні 10 Гбіт/с, то це відповідає сумарній швидкості 6,1 Тбіт/с. Кожний потік 10 Гбіт/с – це при використанні технології SDH (не самої економної) відповідає рівню STM-64, отже це 64х63=4032 потоки Е1, або 120 960 каналів по 64 кбіт/с. Отже, в сумі можна забезпечити 73 785 600 каналів.

Таблиця 4.5 – Позначення та межі оптичних діапазонів

Смуга		Діапазон, нм
Позначення	Назва	
O	Original	1260÷1360
E	Extended	1360÷1460
S	Short wave length	1460÷1530
C	Conventional	1530÷1565
L	Long wave length	1565÷1625
U	Ultra long wave length	1625÷1675

Слід зазначити , що сітка 100 ГГц забезпечує можливість організувати ефективне передавання цифрових потоків у каналах на швидкостях 2,4 Гбіт/с (STM-16) (рис. 4.15а) і 10 Гбіт/с (STM-64) (рисунок 4.15б).

Мультиплексування каналів STM-64 з інтервалом 50 ГГц є недопустимим, оскільки виникає перекриття спектрів сусідніх каналів (рисунок 4.15б)

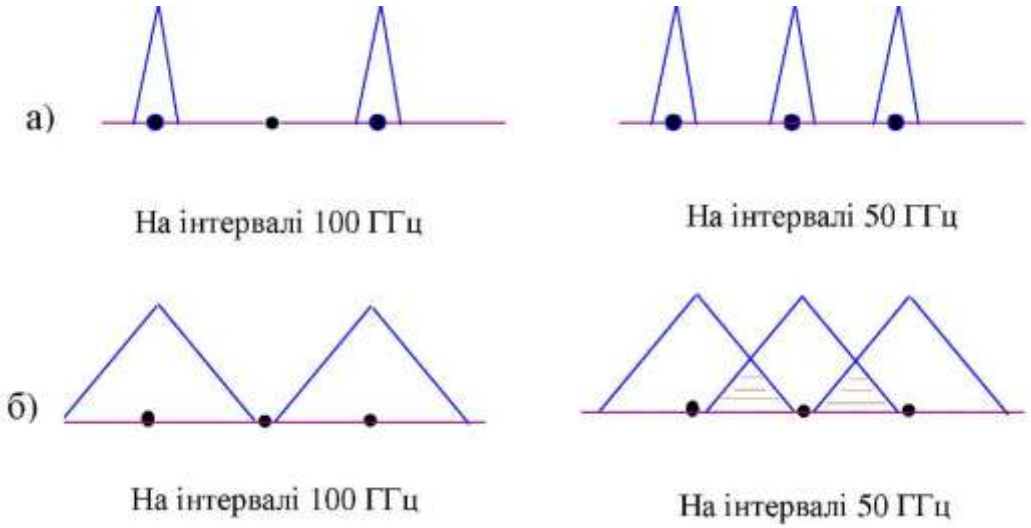


Рисунок 4.15 – Спектральне розміщення каналів у волокні

Основним пристроєм, що відрізняє WDM системи є ***мультиплексор WDM***. Типову схему мультиплексора DWDM/демультиплексора наведено на рисунку 4.16.

Розглянемо роботу DWDM мультиплексора в режимі демультиплексування. Надісланий мультиплексний сигнал потрапляє на вхідний порт. Потім проходить через хвилевід-пластину й розподіляється по хвилеводах, які формують дифракційних структуру. У кожному з хвилеводів дифракційної структури сигнал, як і раніше, залишається мультиплексний. Далі відбувається відбиття сигналів від дзеркальної поверхні, нарешті світлові потоки знову збираються в хвилеводі-пластині, де відбувається їх фокусування та інтерференція – утворюються просторово рознесені інтерференційні максимуми інтенсивності, які відповідають різним каналам. Геометрія хвилеводу-пластини, зокрема розташування вихідних полюсів, і довжини хвилеводів дифракційної структури розраховано таким чином, щоб інтерференційні максимуми збігалися з вихідними полюсами. Мультиплексування відбувається в зворотній послідовності.

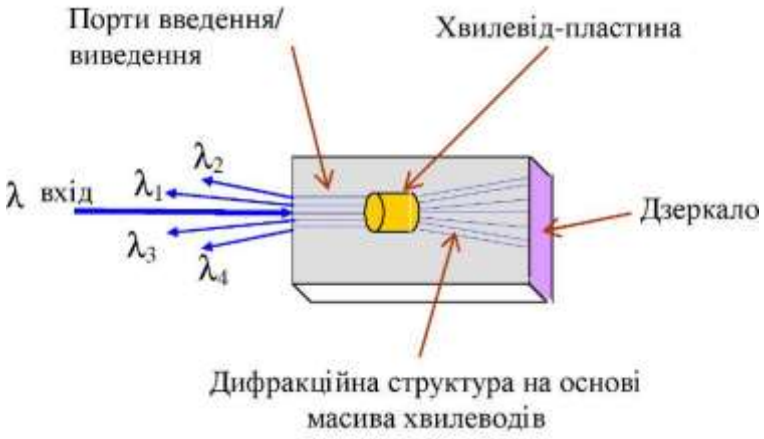


Рисунок 4.16 – DWDM мультиплексор

Разом з пристроями DWDM, у яких мультиплексуються/ демультиплексуються відразу всі канали, впроваджують також нові пристрої, які не мають аналогів у системах WDM і працюють у режимі додавання або вилучення одного та більше каналів основного мультиплексного потоку. У зв'язку з тим, що вихідні порти демультиплексора закріплено за певною довжиною хвиль, говорять, що такий пристрій здійснює *пасивну маршрутизацію* по довжинах хвиль.

DWDM мультиплексори є пасивними пристроями, і вносять велике загасання в сигнал, а тому виникає необхідність встановлення оптичного підсилювача EDFA перед і/або після DWDM мультиплексора.

Для проведення тестів на взаємну сумісність обладнання різних виробників необхідною є стандартизація просторового розташування каналів у волокні.

4.3. Асинхронний метод перенесення інформації

4.3.1. Принципи функціонування систем ATM

Технологія ATM (Asynchronous Transfer Mode) є єдиною технологією, яка дає змогу повноцінно передавати інтегральний трафік (голос, відео, дані), одночасно задовольняючи абсолютно несумісні вимоги до умов передавання.

Асинхронний метод перенесення інформації ATM відіграє одну з центральних ролей в структурі існуючих мереж. Він має ряд важливих переваг перед технологіями передавання даних у локальних і глобальних мережах і дає змогу реалізувати на високих швидкостях ефективне передавання відеоінформації, комп'ютерних даних і мовних сигналів одночасно однією фізичною лінією зв'язку. Це один можливих методів побудови локальних мереж і об'єднання офісів у корпоративні мережі з інтеграцією послуг. Метод ATM забезпечує роботу з усіма типами мережного трафіка, розподіляючи їх цифрові потоки на окремі комірки (пакети).

Керуюча інформація забезпечує визначення типу трафіку і його пріоритету, цілісності комірки та її маршрутизації. Трафік, що направляється комутаторами, може передаватися частинами або повністю. Комутатори можуть відправляти дані будь-яким доступним фізичним шляхом, що значно підвищує швидкість передавання. Протоколи АТМ орієнтовані на попереднє встановлення з'єднань з підтриманням постійного віртуального з'єднання. При цьому в користувача формується ілюзія виділеного каналу, який з'єднує дві кінцеві точки (віртуальні з'єднання). Попри цієї ілюзії в АТМ-мережах користувачі звільняються від оплати виділених ліній, які часто є незайнятими.

Транспортування всіх видів інформації пакетами фіксованої довжини в 53 байта, з яких 48 байтів складають інформаційне поле, а 5 байтів відводиться для заголовка. Такий пакет отримав назву "комірка" (cell). Комірки передаються без додаткового оформлення в кадр (фрейм), а для їх обробляння використовують більш прості протоколи, на відміну від передавання пакетами за протоколом X.25. Крім того, фіксована довжина й регулярність створюваного ними потоку не вимагають використання прапора між ними для відокремлення однієї комірки від іншої. Комірки фіксованої довжини передаються каналом безперервно.

Заголовок містить інформацію для маршрутизації комірки в мережі. Поле даних несе корисну інформацію, яку й потрібно передати мережею. Мережні пристрої АТМ аналізують інформацію в заголовку та вибирають спосіб і шлях проходження комірки мережею. Вони не аналізують вмісту поля даних, який є суттєвим лише для допоміжних програмних продуктів.

У тому випадку, коли інформаційні комірки відсутні, каналом передаються "порожні" комірки стандартної величини, тобто комірки, які не містять даних у полі інформації, що зазначено в заголовку. Порожні комірки необхідно передавати для того, щоб не порушити покоміркову синхронізацію в каналі. Покоміркова синхронізація є аналогом часової дискретизації в синхронному режимі передавання. Однак, якщо у синхронному режимі тривалість тайм-слоту (часового каналу) залежала від швидкості передавання бітів каналом, то в асинхронному режимі тривалість часу, витрачена для передавання комірки, залежить тільки від кількості бітів, необхідних для її передавання, але не від швидкості. Таким чином, за допомогою комірок здійснюється своєрідна «часова дискретизація в каналі», у зв'язку з чим асинхронний режим передавання ще називають асинхронним часовим мультиплексуванням.

Фіксована довжина комірки дає змогу здійснювати надшвидкісну обробку сигналів у комутаторах. За необхідності забезпечити рівномірний трафік, що передаватиметься в реальному масштабі часу (наприклад для відеоконференції), це здійснюється шляхом надання відповідним коміркам пріоритету, про що зазначається у заголовку комірки, а невеликий її розмір сприяє цьому.

АТМ – це яскравий приклад інтеграції систем передавання та комутації, що надає можливість створення потужної єдиної транспортної

мережі для передавання й розподілу інформації будь-якого виду. Основні переваги методу АТМ наступні:

– єдиний універсальний пакет АТМ стикується з багатьма типами служб – відео, передавання даних і мови;

– інфраструктура організації мережі незалежна від надаваних послуг;

– за допомогою АТМ ширина смуги каналу (рисунок 4.17) адаптується до потреб користувачів і динамічно пристосовується до задоволення змінних характеристик трафіка, що надає широкі можливості для найкращого використання пропускної спроможності мережної смуги;

– крім збільшеної пропускної спроможності, АТМ сприяє автоматизації оброблення трафіку, керування мережею та ін.;

– за допомогою технології АТМ створюється більш економічна мережа.

Відмінність асинхронного часового мультиплексування (АЧМ) від синхронного часового мультиплексування (СЧМ) полягає в тому, що комірки, які належать різним інформаційним повідомленням, можуть слідувати довільно, а тайм-слоти СЧМ для передавання різних повідомлень розташовуються на осі часу (в структурі кадру) в чітко фіксованому порядку відносно початку циклу дискретизації (початок кадру) (рисунок 4.18).

Для розміщення корисного інформаційного навантаження, наданого джерелом, у комірках АТМ потрібна його адаптація до вимог перенесення в АТМ шляхом поділу на 48-байтові блоки і подальшим розбиранням цих блоків.

У поле корисного навантаження інформація вводиться динамічно залежно від діючого трафіка, фактично виробленого джерелом. Наслідком цього є те, що ресурси мережі використовуються лише в разі потреби. У цьому полягає відмінність АТМ від синхронних технологій. Комірки, утворені різними передавачами, мультиплексуються в ланцюжки, як правило, з високою фізичною бітовою швидкістю. Результат мультиплексування – це нескінченна послідовність комірок.

Оскільки процес надходження інформації від різних джерел є випадковим, то мультиплексування досягається засобами черг. Черга – це суттєва ознака, яка зумовлює всі властивості АТМ. Всі джерела інформації мережі АТМ фактично стоять у черзі. Черга має певну довжину і може переповнюватися, коли надходить надто інтенсивний трафік, який перевищує очікувані межі. Це спричиняє втрату комірки одного або більше з’єднань, яка пересувається чергою. Практично мережа АТМ допускає таку довжину черги, яка робить імовірність згаданої події незначною, тобто меншою від заданої величини.

Це означає, що будь-який комутатор АТМ містить черги, а велика різноманітність архітектури має оптимізувати затримку і вартість. До складу вузла керування комутатора входить таблиця відповідності, яка завантажена при встановленні з’єднань, і використовується для маршрутизації вхідних комірок до різних вихідних інтерфейсів. Порожні комірки вилучаються на

вході і не надходять до комутатора. Якщо немає інформації, то порожні комірки формуються і на виході.

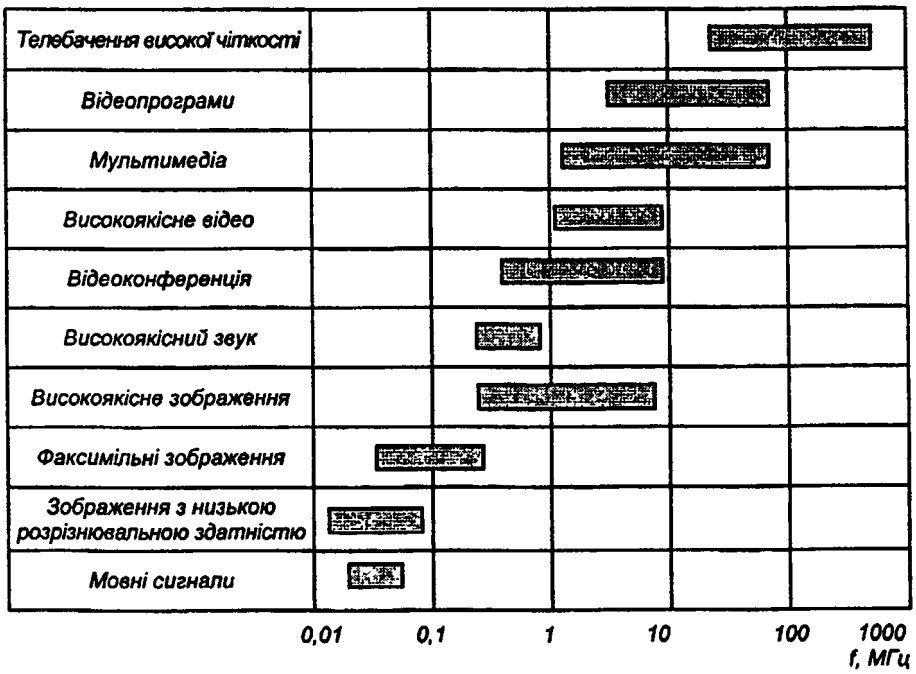


Рисунок 4.17 – Ширина смуги пропускання, що необхідна для різних служб

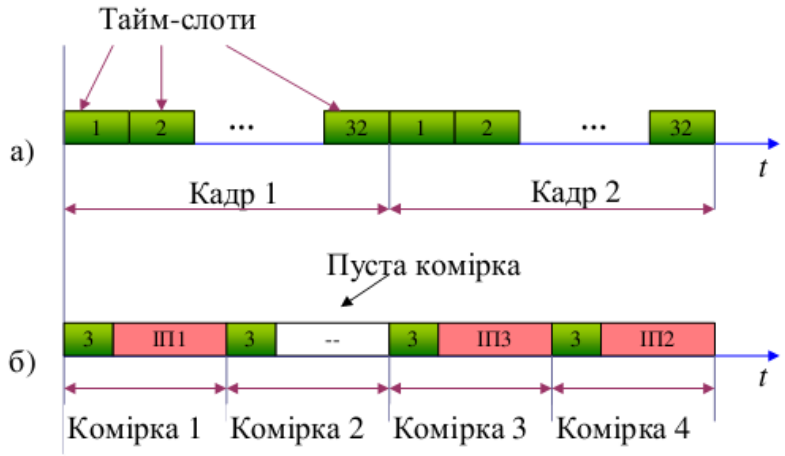


Рисунок 4.18 – Принцип асинхронного мультиплексування:
а - синхронне мультиплексування; б – асинхронне мультиплексування
ІП1, ІП2, ІП3 - інформаційні повідомлення.

Передавання комірок мережею здійснюється завдяки віртуальному з'єднанню, у зв'язку з чим фазі передавання передує фаза налаштування віртуального з'єднання, під час якої перевіряється достатність обсягу мережних ресурсів як для якісного обслуговування вже наявних віртуальних з'єднань, так і для новостворюваного. Якщо мережних ресурсів недостатньо, налаштування з'єднання не відбудеться. Таким чином, у мережі АТМ реалізується функція контролю й захисту від перевантажень. Щоб зменшити часові затримання комірок у вузлах комутації, функції заголовка пакету АТМ обмежують. Основною функцією заголовка стає ідентифікація віртуального

з’єднання та забезпечення гарантії правильної маршрутизації. Заголовок також дає змогу мультиплексувати різні віртуальні з’єднання в одному цифровому тракті. Оскільки помилка в заголовку може призвести до неправильної маршрутизації, передбачено виявлення й виправлення помилок у заголовку пакету АТМ.

Через обмеження функцій, які виконує заголовок пакета АТМ, його обробка є відносно простою процедурою й може здійснюватися на дуже високих швидкостях, що забезпечує незначне затримування комірок у чергах буферних пристроїв комутаторів АТМ. Продуктивність комутаторів АТМ досягає 10 Гбіт/с.

В залежності від ідентифікатора комірки можливі два типи віртуальних з’єднань: шлях (VPI), та канал (VPI+VCI). Віртуальний шлях містить певну кількість віртуальних каналів і тракт передавання може мати декілька віртуальних шляхів (від потрібної пропускної здатності). У випадку віртуального шляху пакети переміщуються за типом “з кінця – у кінець” усередині віртуальних шляхів, зберігаючи свій ідентифікатор. У випадку віртуального каналу досягається послідовність фізичних ланок між вузлами мережі. Віртуального з’єднання можна досягти двома шляхами: оператором мережі з центру керування (це напівпостійні, випадкові або резервні з’єднання; вузол є крос-конектором) та самими користувачами (у реальному часі і для певної тривалості) з використанням спеціальної мови сигналізації.

4.3.2. Сутність технології АТМ

Технологія АТМ (рисунок 4.19) передбачає транспортування всіх видів інформації пакетами (комірками) фіксованої довжини, коли їх потоки від різних користувачів асинхронно мультиплексуються в єдиному цифровому тракті. За протокольну одиницю в АТМ прийнято пакет фіксованої довжини, до якого входять заголовок та інформаційне поле. Застосування коротких пакетів (53 байти), мінімізація виконуваних під час комутації функцій та використання елементної бази за технологіями інтегральних схем і великих інтегральних схем уможливили досягнення продуктивності комутаторів АТМ 10 Гбіт/с і більше.

Основною позитивною рисою методу АТМ є можливість транспортування інформації незалежно від швидкості передавання, вимог до семантичної й часової прозорості мережі та пульсування коміркового трафіка. Це зумовило появу рішення Міжнародної спілки електрозв’язку про те, що АТМ є режимом транспортування інформації для широкосмугової цифрової мережі з інтегральним обслуговуванням (ШЦМІО).

Саме технологія АТМ забезпечує гнучкість мережі, ефективність використання мережних ресурсів та можливість створення єдиної універсальної мережі для всіх нинішніх і майбутніх служб. Технологія АТМ підтримується будь-якою цифровою системою передавання, тому що створює протоколи на рівнях, вищих від фізичного.

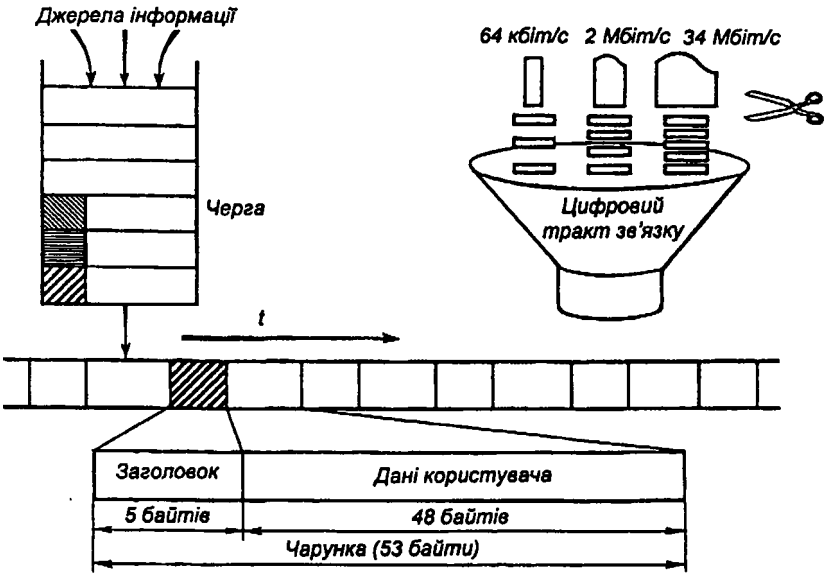


Рисунок 4.19 – Сутність технології АТМ

Гнучкість мережі забезпечується завдяки тому, що будь-яке джерело може генерувати інформацію з потрібною швидкістю. Це дає змогу постійно удосконалювати алгоритми кодування та стиснення інформації для зменшення необхідної смуги пропускання і появи нових служб.

Наявні ресурси мережі можуть використовуватися всіма службами, а це уможливлює їх оптимальний розподіл за статистичною основою, отже, дає змогу забезпечити високу ефективність використання мережних ресурсів.

Транспортування різних видів інформації одним методом обумовлює проектування, створення, впровадження в експлуатацію, контроль, керування і технічне обслуговування лише однієї мережі, що скорочує загальні витрати на її створення і робить її найбільш економічною мережею електрозв’язку.

Асинхронний метод перенесення інформації характеризується відсутністю захисту від помилок і керування потоком даних на однакові ланки, орієнтацією на з’єднання, обмеженою кількістю функцій, які несе заголовок пакета АТМ, та відносно невеликою довжиною інформаційної частини комірки. Висока якість систем передавання цифрових трактів зв’язку і дуже низька ймовірність помилки за біт дають змогу відмовитися від виявлення та виправлення помилок у пакеті на канальному рівні.

Щоб уникнути перевантажень, на рівні ланки немає керування потоком даних. Фазі передавання інформації в мережах АТМ передує фаза встановлення віртуального з’єднання, під час якого перевіряється достатність обсягу мережних ресурсів для якісного обслуговування встановлених і створюваних віртуальних з’єднань. Якщо мережних ресурсів недостатньо, то кінцевому пристрою видається відмова на встановлення з’єднання. Після закінчення фази передавання інформації віртуальне з’єднання руйнується, а мережні ресурси можуть використовуватися для забезпечення іншого віртуального з’єднання. Отже, завдяки режиму перенесення інформації, орієнтованого на з’єднання і визначення розмірів черг, здійснюється контроль за втратами пакетів через переповнення буферних пристроїв

комутаторів. У мережах АТМ імовірність втрати пакета в комутаційному пристрої становить $10^{-8}…10^{-11}$.

Для зменшення часу затримання пакета у вузлах комутації функції пакетного заголовка дуже обмежені. Основною його функцією є ідентифікація віртуального з'єднання за допомогою ідентифікатора і забезпечення гарантії правильної маршрутизації. Заголовок також уможливлює мультиплексування різних віртуальних з'єднань в одному цифровому тракті. Помилка в заголовку може призвести до неправильної маршрутизації, що зумовлює ефект розмноження помилок: один спотворений біт у заголовку може зумовити втрату пакета або доставлення його не за адресою. Щоб зменшити ефект розмноження помилок через неправильну маршрутизацію, в заголовку пакета АТМ передбачається їх виявлення та виправлення.

Через обмеженість функцій, виконуваних заголовком, обслуговування пакета АТМ вважається досить простою процедурою, що здійснюється на надвисоких швидкостях, які забезпечують незначне затримання пакетів у черзі буферних пристроїв комутаторів АТМ.

Малі розміри інформаційного поля зумовлюють незначну тривалість затримки на пакетизацію, що разом з відносно невеликими розмірами буферних пристроїв вузлів комутації, які забезпечують незначне затримання і коливання затримки, характеризує часову прозорість мереж АТМ для служб, які функціонують у реальному масштабі часу.

Мережа АТМ, яка спроможна транспортувати єдиним методом усі види інформації, забезпечує:

– високу гнучкість і адаптацію щодо зміни вимог користувачів до обсягу, швидкості, якості доставляння інформації та щодо появи вимог про надання нових послуг, які потребують наявності в мережі інтелекту;

– підвищення ефективності використання мережних ресурсів внаслідок статистичного мультиплексування множини джерел з пакетним трафіком;

– зниження загальних витрат на проектування, будівництво й експлуатацію мережі.

Проте основною проблемою, що виникає в мережах АТМ, є задоволення вимог різних служб до часової й семантичної прозорості мережі та їх адаптації до єдиного методу перенесення.

Комутатори АТМ є основними пристроями мережі АТМ, основними функціями яких є не тільки налаштування віртуального з'єднання між кінцевими пристроями користувачів, а й забезпечення так званого режиму якісного обслуговування (Quality of Service, QoS) для цього з'єднання. Параметри режиму QoS задають користувачі в заявці на під'єднання в фазі формування віртуального з'єднання.

У рекомендаціях ITU-T передбачено такі типи QoS:

– CBR (Constant Bit Rate) – створення каналу з фіксованою пропускною здатністю, гранично допустимим затримуванням та іншими

характеристиками, замовленими користувачем. Такий вид QoS в основному використовують для передавання мовлення;

– RT-VBR (Real Time Variable Bit Rate) – створення каналу з пропускною здатністю в заданих межах (min-max) з жорсткими вимогами до затримування та іншими параметрами, замовленими користувачем. RT-VBR є ідеальним для передавання відео й мовлення;

– NRT-VBR (Not Real Time Variable Bit Rate) – VBR з послабленими вимогами до затримування у передаванні – застосовується для відео та мовлення, які не потребують режиму реального часу;

– ABR (Availeble Bit Rate) – надання користувачеві залишково вільної частини фізичного каналу. Під'єднуючись, користувач встановлює лише межі допустимих змін швидкості передавання. Величина затримувань є контрольованою. Даний режим застосовують для передавання даних;

– UBR (Unspecified Bit Rate) – найбільш низькопріоритетний режим передавання, особливість якого в тому, що надається для користування певний канал без будь-яких гарантій якості передавання;

– UBR+ – модифікований UBR, який передбачає припинення передавання комірок повідомлення у разі виникненні перевантаження мережі. Застосування UBR + дає змогу розвантажити фізичні канали.

Забезпечення режиму QoS принципово відрізняє технологію ATM від усіх наявних мережних технологій. Особливого значення вона набуває в процесі інтегрування даних відео й мовлення, надзвичайно чутливих до затримування під час передавання.

Єдиним протоколом, який забезпечує QoS у комутаторах ATM, є протокол PNNI Phase 1.0 (Private Network – to – Network Interface). Протокол досить складний, для його роботи потрібно вдесятеро більше процесорного часу, ніж, наприклад, для відомого протоколу визначення найкоротшого шляху (OSPF), який використовується в маршрутизаторах.

4.3.3. Еталонна модель протоколів ATM

В Рекомендаціях Міжнародної спілки електрозв'язку модель ATM описана як складова протоколу ШЦМІО. Дотримуючись Рекомендацій Міжнародної спілки електрозв'язку (модель протоколів ШЦМІО є розподілом моделі, описаної в Рекомендації I.320), подамо загальний вигляд еталонної моделі протоколів за технологією ATM (рисунок 4.20). До складу моделі входять три площини: площина користувача, площина керування і площина менеджменту.

Площина користувача (U-plane) забезпечує транспортування всіх видів інформації разом з механізмами захисту від помилок, контролю і керування потоком, обмеження навантаження тощо. Площина користувача має рівневу структуру. *Площина керування* (C-plane) визначає протоколи встановлення, контролю і роз'єднання зв'язку, їй належать усі функції сигналізації, крім протоколів метасигналізації. Площина керування також має рівневу структуру. *Площина менеджменту* (M-plane) забезпечує виконання функцій

двох типів – менеджменту (керування) площинами і менеджменту (керування) рівнями.

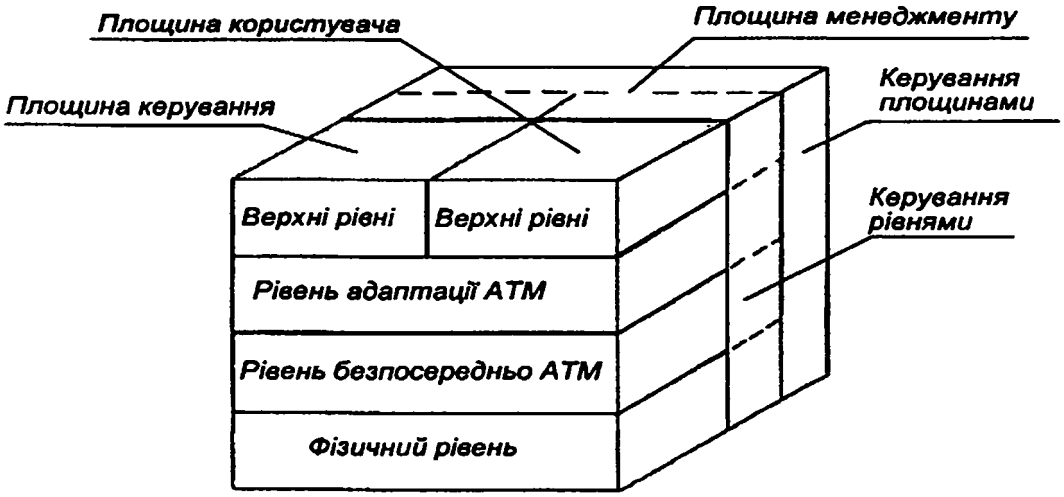


Рисунок 4.20 – Еталонна модель протоколів за технологією ATM

Функції керування площинами передбачають координацію протоколів між усіма «гранями» моделі, зв'язуючи її в одне ціле. Ділянка керування площинами не має рівневої структури. Функції керування рівнями забезпечують розподіл мережних ресурсів, узгодження їх з параметрами трафіка, оброблення інформації, експлуатацію й технічне обслуговування мережі, керування нею. Процедури метасигналізації також належать до функцій керування рівнями.

Ділянка керування рівнями має рівневу структуру. Рівні еталонної моделі протоколів ATM визначені Рекомендаціями I.321 і I.413. На даний час детально обґрунтовані функції тільки перших трьох рівнів моделі, якими є фізичний, безпосередньо ATM, де структуруються комірки, та адаптації ATM, який підтримує послуги верхніх рівнів (емуляцію каналів, високошвидкісне передавання даних без встановлення з'єднання, ретрансляцію кадрів тощо).

Фізичний рівень моделі протоколів ATM відповідає 1-му (фізичному) рівню еталонної моделі OSI, ***рівень безпосередньо ATM*** і частина ***рівня адаптації ATM*** – 2-му (канальному) рівню OSI, а верхні рівні – мережному і вищим рівням OSI. На рисунку 4.21 показано співвідношення рівневих структур ATM та еталонної моделі OSI, а також поділ рівнів ATM на підрівні (таблиця 4.6).

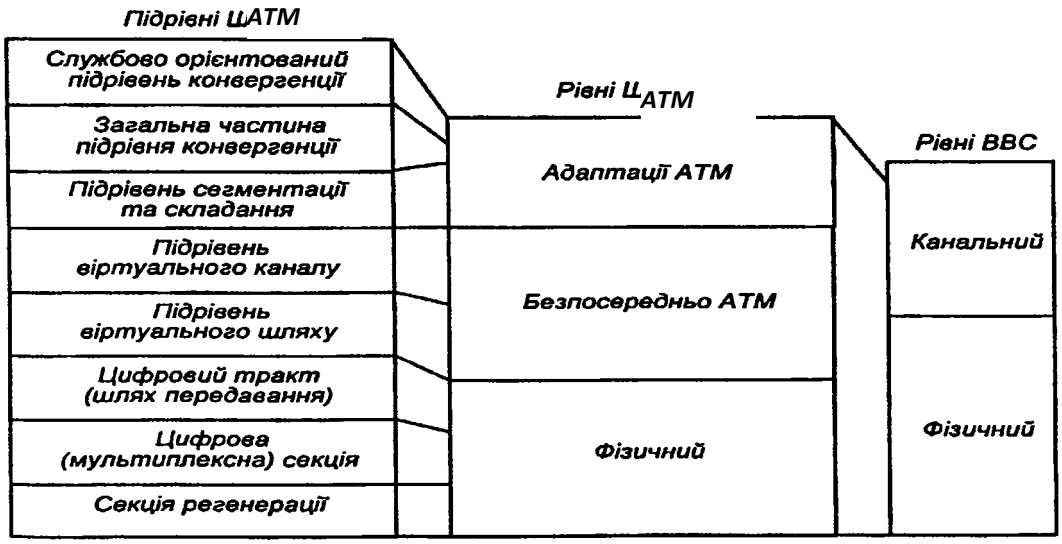


Рисунок 4.21 – Рівні та підрівні АТМ і їх співвідношення з рівнями моделі OSI

Таблиця 4.6 – Функції рівнів та підрівнів АТМ

Рівень	Підрівень	Основні функції
Адаптації АТМ	Конвергенції	Конвергенція до служби
	Сегментації та складання	Сегментація інформації та складання чарунок
Безпосередньо АТМ	Віртуального каналу та віртуального шляху	Загальне керування потоком; генерація та вилучення заголовка чарунки; перетворення ідентифікаторів віртуальних каналів і шляхів; мультиплексування та демультиплексування чарунок
Фізичний	Конвергенції до системи передавання	Узгодження швидкості потоку чарунок; формування поля контролю помилок; виявлення та виправлення помилок; адаптація потоку чарунок до кадру системи передавання та виділення чарунок; генерація кадру системи передавання та відновлення кадру
	Конвергенції до фізичного середовища	Синхронізація; передавання двійкового сигналу в даному середовищі

4.4. Мережі з використанням технології mpls

4.4.1. Технологія MPLS

У середині 90-х років цілком придатною вважалася багаторівнева структура, в якій під рівнем IP передбачено використовувати мережі АТМ і Frame Relay (FR), а на фізичному рівні – SDH/PDH або DWDM. Застосування такої архітектури та ще з двома рівнями передавання пакетів (на канальному з використанням віртуальних каналів і на мережному, в основному, датаграмним способом) робило глобальну мережу дуже складною і дорогою. Проте вважалося, що ці недоліки можна не брати до уваги, оскільки

перевагами були передавання мультимедійного трафіку та забезпечення необхідної якості обслуговування (Quality of Service, QoS).

Новим словом у сфері інтеграції IP з технологіями віртуальних каналів стала технологія мультипротокольної комутації міток. Вона займає проміжне місце між рівнем IP і рівнем таких технологій, як ATM, FR або Ethernet, інтегруючи їх у єдину ефективну технологію.

Багатопротокольна комутація міток (Multiprotocol Label Switching, MPLS) – це технологія магістральних мереж, яка значно підвищує швидкість передавання трафіку територіальних мереж. Термін «багатопротокольна» в назві технології означає, що технологія MPLS застосовується до будь-якого протоколу мережного рівня, тобто, це своєрідний інкапсулювальний протокол, здатний транспортувати інформацію безлічі інших протоколів вищих рівнів моделі OSI. Технологія MPLS є незалежною від протоколів канального й мережного рівнів у мережах IP, ATM і FR, а також взаємодіє з наявними протоколами маршрутизації, такими як протокол резервування ресурсів RSVP або мережний протокол переважного вибору найкоротших маршрутів OSPF.

Положення технології MPLS відносно семирівневої моделі OSI/ISO показано на рисунок 4.22.

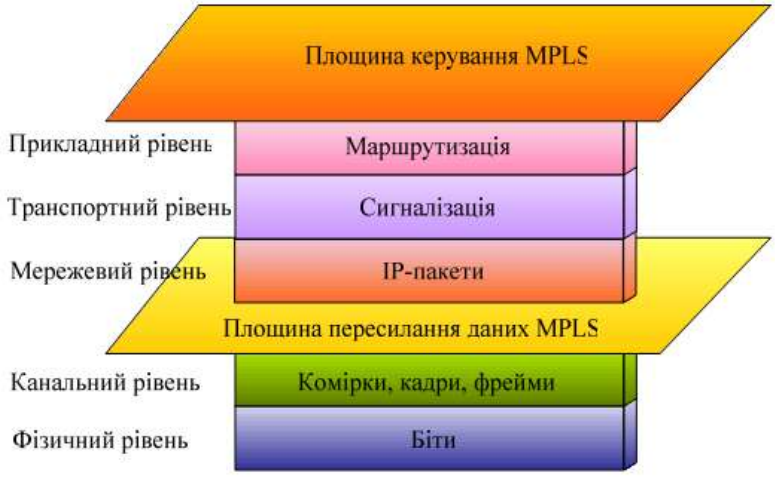


Рисунок 4.22 – Площина MPLS

Площина пересилання даних MPLS не утворює повноцінного рівня, вона "вклинюється" в мережі IP, ATM або FR між 2-м і 3-м рівнями моделі OSI, залишаючись незалежною від цих рівнів. Можна сказати, що можливість функціонування MPLS на мережному й канальному рівнях призводить до утворення так званого рівня 2.5, де, власне, й виконується комутація за мітками.

MPLS поєднала в собі надійність і гарантовану якість обслуговування ATM зі зручними й потужними засобами доставки IP-мереж. Така інтеграція дала змогу отримати додаткову користь від спільного використання протоколів IP та ATM і може розглядатися як гібрид мережі з віртуальними каналами й мережі з пакетною маршрутизацією, яка реалізує стек TCP/IP.

Особливість технології MPLS – це відокремлення процесу комутації пакету від аналізу IP-адреси в його заголовку. Для цього пристрої, які здійснюють комутацію або маршрутизацію, призначають коміркам або пакетам короткі мітки фіксованої довжини. Зазвичай комутація міток реалізується не у всій мережі, а в деякій групі її сегментів, частіше – магістральних. Ця група сегментів називається доменом MPLS (або мережею MPLS). У разі комутації за міткою повний аналіз заголовка третього рівня здійснюється лише один раз – на вході в домен MPLS. Це виконує розташований на межі домену пристрій, який називається прикордонним маршрутизатором з комутацією міток (Label Switch Router, LSR). Далі, всередині домену, проміжні LSR аналізують лише мітки. Це дає змогу передавати пакети всередині домену значно швидше.

Вихідний прикордонний LSR виконує операцію вилучення з пакета мітки, аналізує заголовок пакета й направляє його до адресата, який знаходиться поза MPLS-мережею. Таким чином, привласнення мітки є своєрідною “формою інкапсуляції” пакета, а сам процес проходження пакета через домен MPLS аналогічний до тунелювання. Оскільки заголовок мережного рівня у процесі маршрутизації через домен не враховується, комутацію міток можна використовувати для передавання пакетів не тільки IP, але і будь-яких інших протоколів мережного рівня.

Для технології MPLS визначено чотири основні елементи:

– мітка;
– клас еквівалентності пересилання (FEC);
– комутуємий за мітками тракт (LSP);
– таблиця пересилання.

Розглянемо кожен з них більш детально.

Мітка є спеціальним заголовком – заголовком MPLS розміром 4 байти. При цьому ідентифікатор самої мітки займає перші 20 біт. Мітку можна передавати у складі будь-якого пакета. При цьому, в усіх випадках, коли це можливо, для її розміщення використовуються уже наявні формати пакетів тієї чи іншої технології. З цієї причини розташування мітки в пакеті залежить від застосовуваної технології канального рівня. Вона може бути поміщена в пакет як додатковий заголовок, який розташовується між заголовками рівня 2 і рівня 3, як це показано на рисунку 4.23. У цьому випадку заголовок MPLS часто називають заголовком-клином (shim header), підкреслюючи те, що він "вклинюється" в пакет між заголовками канального й мережного рівня.

Крім того, мітка може бути розміщена у вільне та доступне поле заголовку (якщо таке є) одного із зазначених двох рівнів. Це може бути поле ідентифікатора з’єднання канального рівня для кадру технології FR або поле ідентифікаторів віртуального каналу та віртуального шляху, у разі комірки ATM. Принцип, зображений на рисунку 4.23, підходить для каналів "точка-точка" й для локальних мереж Ethernet усіх типів. Подібним методом можна передати одну MPLS-мітку або стек міток, про який мова піде далі.

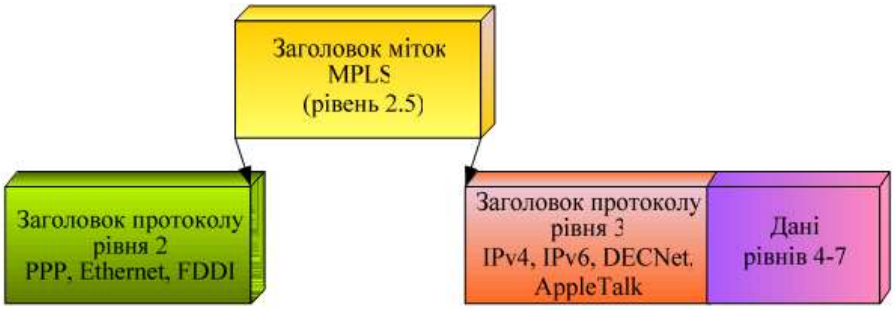


Рисунок 4.23 – Розміщення мітки MPLS

Стек міток. Пакет, який передають через мережу MPLS, як правило, містить не одну, а кілька міток. Такий набір міток утворює стек (рисунок 4.24). Основне призначення стеку міток – підтримка деревоподібності множини трактів LSP, які закінчуються в одному вхідному LSR, а також у тому, щоб використовувати мітки під час створення, так званих, LSP-тунелів. Специфікацію кодування стеку міток MPLS визначено в RFC 3032 “MPLS Label Stack Encoding”. Даний документ містить детальну інформацію про мітки та про те, як вони застосовуються у різних мережних технологіями, а також визначає ключове для технології MPLS поняття – стек міток. Можливість мати в пакеті більше ніж одну мітку у вигляді стеку дає змогу створювати ієрархію міток, яка уможливлює роботу багатьох застосувань.

У MPLS зі стеком можуть виконуватися такі операції: розміщення мітки в стек, вилучення мітки зі стеку й заміна мітки. Операція розміщення мітки в стек (push operation) долучає нову мітку поверх стеку, а операція вилучення мітки зі стеку (pop operation) видаляє верхню мітку зі стеку. Ці операції використовують для злиття та розгалуження інформаційних потоків різних застосувань. Функціональні можливості стеку MPLS дають змогу об’єднувати кілька LSP у один. До стеку міток кожного з цих SP зверху додається загальна мітка, в результаті чого утворюється агрегований тракт MPLS. У точці закінчення такого тракту відбувається його розгалуження на складові індивідуальні LSP. Так можуть об’єднатися тракти, які мають спільну частину маршруту. Отже, MPLS здатна забезпечувати ієрархічне пересилання, що є важливою й потрібною функцією.

Згідно з розглянутими нижче правилами інкапсуляції міток, за міткою MPLS в пакеті завжди має слідувати заголовок мережного рівня. Так як MPLS починає роботу з вершини стеку, використовується процедура Li-Fo “останнім прийшов – першим пішов”. Приклад чотирирівневого стеку міток зображено на рисунку 4.24. Заголовок MPLS № 1 був першим заголовком MPLS, вміщеним у пакет, потім – заголовки № 2, № 3 і, нарешті, заголовок № 4. Комутація за мітками завжди використовує верхню мітку стеку, а мітки видаляють з пакету так, як це визначено вихідним вузлом для кожного LSP, по якому слідує пакет.

Рисунок 4.24 – Чотирирівневий стек міток

Клас еквівалентності пересилання (Forwarding Eguivalency Class, FEC) є групою пакетів мережного рівня, які відправляють один за одним і тим же маршрутом та обслуговуються однаково. Об'єднання пакетів у класи використовують для надання пріоритетів одним групам пакетів (наприклад, мовним) відносно інших для почерговості їх проходження через проміжні комунікаційні пристрої всередині домену. Зарахувавши пакет до того чи іншого класу еквівалентності пересилання, прикордонний маршрутизатор LSR може переглянути IP-заголовок пакета, а також використовувати іншу інформацію, зокрема фізичну адресу (номер інтерфейсу), на який надійшов пакет. Відповідно до просування пакету мережею, кожен наступний LSR аналізує його заголовок і приписує цей пакет до того із власних класів еквівалентності, котрий належать тільки цьому LSR та відповідає тому ж напрямку. На відміну від традиційної маршрутизації, в мультипротокольній комутації на основі міток пакет ідентифікується з певним класом FEC тільки один раз – на вході в мережу MPLS. За цим FEC закріплюється мітка, яку передається потім разом з пакетом у процесі його пересиланні до наступного LSR. У інших LSR заголовок пакета не аналізується.

Комутований за мітками тракт (Label Switch Path, LSP) – це віртуальний комутований за мітками тракт, так званий тунель, який являє собою встановлене логічне з'єднання і є симплексним з'єднанням. Для організації напівдуплексного з'єднання необхідними є два LSP. LSP завжди починається на одному кінці домену MPLS і закінчується на протилежному, проходячи через кілька транзитних пристроїв (LSR).

Таблиці пересилання. У мережі MPLS кожен маршрутизатор комутації за мітками LSR створює таблицю пересилання, за допомогою якої він визначає, яким чином треба пересилати пакет, який до нього надійшов. Цю таблицю називають інформаційною базою міток (Label Information Base, LIB). Вона містить використовувану кількість міток, а для кожної з них – прив'язку "FEC – мітка". В інформаційну базу LIB входить така інформація:

– операція, яку треба виконати зі стеком міток пакета (замінити верхню позначку стеку, вилучити верхню позначку, помістити поверх стеку нову позначку);

– наступний LSR у тракті (LSP);

– використовувана в процесі передавання пакета інкапсуляція на канальному рівні;

– спосіб кодування стеку міток у процесі передавання пакета;
– інша інформація про пересилання пакета.

Таблиця пересилання, яка містить дану інформацію та яку формує LSR, є послідовністю записів. Кожен запис таблиці складається з вхідної мітки та однієї або більше підзаписів, причому кожен підзапис містить значення вихідної мітки, ідентифікатор вихідного інтерфейсу й адресу наступного маршрутизатора в LSP. Приклад простої таблиці пересилання LIB подано на рисунку 5.25.

```
R1#sh mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing   Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  3.3.3.3/32       0             Et0/1      10.0.13.3
17         Pop Label  10.0.34.0/24     0             Et0/1      10.0.13.3
18         16         5.5.5.5/32       0             Et0/0      10.0.12.2
19         Pop Label  2.2.2.2/32       0             Et0/0      10.0.12.2
20         17         10.0.45.0/24     0             Et0/0      10.0.12.2
           23         10.0.45.0/24     0             Et0/1      10.0.13.3
21         Pop Label  10.0.25.0/24     0             Et0/0      10.0.12.2
23         20         4.4.4.4/32       0             Et0/1      10.0.13.3
25         26         10.0.56.0/24     0             Et0/0      10.0.12.2
26         27         6.6.6.6/32       0             Et0/0      10.0.12.2
```

Рисунок 5.25 – Таблиця пересилання LIB

Різні підзаписи всередині одного запису можуть мати або однакові, або різні значення вихідних позначок. Більше ніж один підзапис буває потрібним для підтримки багатоадресного розсилання пакету, коли пакет, який надійшов до одного вхідного інтерфейсу, треба потім розсилати через кілька вихідних інтерфейсів. Звернення до конкретної запису в таблиці здійснюють за значенням вхідної мітки. Запис у таблиці може також містити інформацію, що вказує, які ресурси має можливість використовувати пакет, наприклад певну вихідну чергу.

LSR може підтримувати або одну загальну таблицю, або окремі таблиці для кожного зі своїх інтерфейсів. У першому варіанті обробляння пакета визначається тільки міткою, яку переносить пакет. У другому варіанті обробляння пакета визначається не тільки міткою, а й інтерфейсом, до якого надійшов пакет. LSR може використовувати або перший варіант, або другий, або їх поєднання.

Прив'язка "мітка-FEC". Кожен запис у таблиці пересилання, яку веде LSR, містить одну вхідну мітку й одну або більше вихідних. Згідно з цими двома типами міток, забезпечуються два типи прив'язки міток до FEC:

– перший тип – мітка для прив'язки вибирається й призначається у LSR локально. Таку прив'язку називають локальною;

– другий тип – LSR отримує від іншого LSR інформацію про прив'язку мітки, яка відповідає прив'язці, створеній на цьому іншому LSR. Таку прив'язку називають віддаленою.

Засоби керування комутацією за мітками використовують для заповнення таблиць пересилання як локальну, так і віддалену прив'язку міток

до FEC. Це може здійснюватися в двох варіантах. Перший: коли мітки на локальній прив'язці використовують як вхідні мітки, а мітки з віддаленої прив'язки – як вихідні. Другий варіант – прямо протилежний, тобто мітки з локальної прив'язки використовують як вихідні мітки, а мітки з віддаленої прив'язки – як вхідні.

Однією з найсильніших сторін технології MPLS є те, що її можна використовувати спільно з різними протоколами канального рівня. Серед цих протоколів – ATM, FR, PPP і Ethernet, FDDI та інші, передбачені документами щодо MPLS. Використання MPLS поверх ATM є досить активним, особливо для транспортування мережами ATM трафіку IP. ATM-комутатори, конфігуровані для підтримки MPLS (ATM-LSR), виконують протоколи маршрутизації TCP/IP і використовують пересилку даних комірками фіксованої довжини – 53 байти. Усередині цих ATM-LSR верхня мітка MPLS поміщається у поле ідентифікаторів віртуальних каналів у заголовку комірки ATM, а дані про стек міток MPLS – у поле даних комірок ATM. MPLS у мережах Frame Relay започатковано багатьма постачальниками послуг, і до цього часу широко використовується. Подібно до ATM, FR-комутатори, які підтримують MPLS, застосовують протоколи маршрутизації TCP/IP для пересилання даних під керуванням FR. MPLS дає змогу створювати нові формати міток без зміни протоколів маршрутизації, а тому впровадження цієї технології в новостворені види оптичного транспорту, такі, як щільне мультиплексування з розподіленням за довжиною хвилі DWDM (Dense Wave Division Multiplexing) і оптична комутація, є відносно простим завданням. Використання MPLS у мережах Ethernet, особливо в міських мережах, є ще однією перспективною можливістю. У стандарт Ethernet вносяться зміни, які дають змогу збільшити швидкість і дальність передавання Ethernet-пакетів. У даний час починають застосовувати Ethernet-інтерфейси на швидкостях 10 Гбіт/с, а незабаром з'являться Ethernet-інтерфейси на ще вищих швидкостях.

4.4.2. Технологія GMPLS

Технологія узагальненої мультипротокольної комутації за мітками (Generalized Multi-Protocol Switching, GMPLS) використовує концепцію й протоколи, розроблені для MPLS, однак принцип комутації за мітками тут поширено також на оптичні мережі. Технологію GMPLS розроблено технічною комісією Інтернету (Internet Engineering Task Force, IETF).

У GMPLS, разом з міткою, необхідно передавати інформацію про її тип, тому що у якості міток можуть використовуватися різні компоненти: довжина хвилі, номер оптичного волокна в каналі, номер SDH-контейнера та ін. На даний момент базовими типами міток є:

- Packet – мітка, яка ідентифікує Ethrnet (GT, FE);
- PDH – мітка, яка ідентифікує кадри (T1, E1, E3);
- SONET/SDH – мітка, яка ідентифікує контейнери SDH (STM-n);
- Digital Wrapper – мітка OTH G.709 (2.5, 10, 40 Гбіт/с);

– λ – довжина хвилі при використанні фотонних комутаторів;
– Fiber – мітка, яка ідентифікує номер оптичного волокна;
– Fiber Channel – мітка, яка ідентифікує оптичний канал.

Наведені вище мітки вказують тип налаштованого з'єднання LSP, а не транспортну технологію, скрізь яку воно утворюється. Технологія GMPLS має чимало цікавих властивостей, серед яких особливо прикметними є такі:

– можливість налаштовувати та обслуговувати з'єднання, які організовуються скрізь різні технологічні рівні мережі;
– автоматичне розпізнавання мережних ресурсів;
– автоматична інвентаризація (відстеження зміни та облік) мережних ресурсів;
– реалізація інтелектуальних захисних механізмів.

GMPLS охоплює весь комплекс комутаційних можливостей – від комутації пакетів до комутації оптичних волокон через IP-маршрутизатори, Ethrnet-комутатори, оптичні мультиплексори введення/виведення, закінчення систем WDM. Вона еволюціонувала від MPLS і базується на тих самих протоколах маршрутизації та сигналізації. Тим самим забезпечується гнучка взаємодія між традиційними та новостворюваними магістральними інфраструктурами. Розширені можливості QoS у GMPLS дають змогу ефективно передавати через єдину мережу повідомлення з різними класами сервісу, такі, як голос, відео та дані з їх специфічними вимогами до затримувань та тремтіння фази. Гнучке та ефективне мережне управління, пропоноване GMPLS, уможливлює швидке й просте залучання нових транспортних послуг.

4.4.3. Мультисервісні транспортні мережі

Як випливає з попередньої інформації, транспортна мережа в загальному випадку – це сервісна платформа, створена ресурсами первинної та базових сервісних мереж. Первинна мережа будується з використанням технологій та комунікаційного устаткування фізичного рівня на основі розподільчих середовищ, а базові сервісні мережі – з використанням технологій та обладнання канального рівня на основі комутованої топології. Транспортні можливості такої сервісної платформи, як правило, визначаються технологічними особливостями базових сервісних мереж. Усі базові сервісні мережі транспортних мереж METRO взаємодіють на основі протоколу мережного рівня IP, утворюючи сегмент наступного ієрархічного рівня – транспортну мережу CORE.

Процеси конвергенції базових сервісних мереж, а також інтеграція їх з первинною мережею (фізичним рівнем) створили передумови для побудови єдиної мультисервісної транспортної мережі на основі уніфікованих мережних рішень.

Мультисервісною транспортної мережею (Multiservice Transport Network, MTN) називається мережа, яка забезпечує надання різних транспортних послуг з використанням найбільш придатної мережної

технологій та відповідних мережних ресурсів з передбачуваною якістю і за наявності різних технологій доступу.

Транспортні послуги мультисервісної мережі – це забезпечення гарантованого сервісу при транспортуванні потоків будь-яких видів даних, що виникають при наданні користувачам інфокомунікаційних послуг з необхідною якістю. Упровадження нових інфокомунікаційних послуг, які, в основному, пакетно-орієнтовані та широкосмугові (IPTV, відеоконференції, відеоігри "on-line"), призводить не тільки до значного збільшення трафіку, але й до значного зростання вимог до масштабованості пропускної здатності транспортних мереж. Така мережа повинна містити будівельні блоки, які забезпечують транспортування як уніфікованих транспортних потоків, так і потоків трафіку різних сервісів з передбачуваною за будь-яких умов якістю. Для досягнення цього, специфічні функції захисту (виявлення та інформування про помилки) повинні бути реалізовані не тільки в кінцевих точках термінування трафіку, але й у кожному мережному вузлі транспортної мережі.

Мультисервісність знижує конкурентноздатність окремих базових сервісних мереж, що змушує мережних операторів модернізувати свої телекомунікаційні інфраструктури. Розглядаючи еволюцію від TDM до пакетного мультиплексування, слід враховувати, що мережа, оптимізована для однієї задачі, може виявитися не зовсім вдалою для іншої. Або мережа, побудована з досить низькими капіталовкладеннями, може вимагати високих вкладень у експлуатацію та виявитися непристосованою для надання сервісів із заданою якістю. Однак у будь-якому випадку витрати на реконструкцію мережі повністю покриваються за рахунок досягнення підвищеної гнучкості мережі. А завдяки оптимізованому розподілу ресурсів і ефективним механізмам відновлення, можна значно знизити експлуатаційні витрати, що в результаті збільшує прибутки.

Мультисервісна мережа є невід’ємною складовою мереж наступного покоління (Next Generation Network, NGN). Якщо NGN – це концепція надання послуг, то мультисервісність – технологія побудови транспортної мережі. Основне призначення мультисервісних технологій полягає в тому, щоб забезпечити гнучку модернізацію транспортної мережі для наданні наявних та перспективних послуг. Мультисервісна платформа надання послуг (Multiservice Provisioning Platform, MSPP) є основою побудови мереж NGN. Вона є злиттям у єдину уніфіковану інтелектуальну мультисервісну транспортну мережу численних мережних інфраструктур, таких як: SDH із передаванням поверх неї пакетизованих даних (G.707, G.7041, G.7042), OTP (G.709), систем з поділом каналів за довжиною оптичного випромінювання (WDM, DWDM) і технології GMPLS.

Останні досягнення в SDH пов’язано з упровадженням концепції MSPP (NG SDH), у якій звичайні для SDH функції керування смугою синхронного транспорту об’єднано в тому ж обладнанні з функціями асинхронної комутації та передавання пакетного трафіку Ethernet. Успіх упровадження платформ MSPP засновано на їх здатності ефективно підтримувати щораз

більші потоки пакетного трафіку, які постійно збільшуються з обробляннням та перемиканням його в початковій формі та передаванням спільно з TDM трафіком. Компанія

Alcatel була першою серед тих, хто впровадив мультисервісні вузли платформи MSPP. У новому сімействі обладнання – транспортних сервісних комутаторах – функції обробляння (які залежать від технології, наприклад пакети або канали TDM, або оптичні λ-канали) й перемикання трафіку (на основі технологій побудови комутаційних блоків) розділено. У результаті створено ідеальну конвергентну платформу як для традиційних TDM, так і нових пакетно-орієнтованих IP/Ethernet сервісів (рисунок 4.26). Крім того, це сімейство інтегрує в собі технології WDM та DWDM, а також GMPLS. Це дає змогу операторові самому вирішувати, з урахуванням пропонованих вимог, чи передавати оптичним волокном Ethernet трафік у своїй натуральній формі або, після агрегування, поверх SDH.

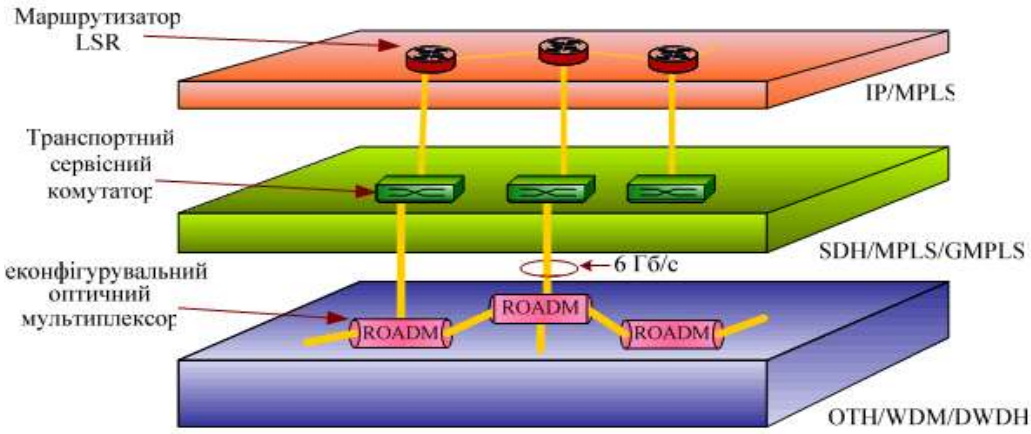


Рисунок 4.26 – Архітектура платформи MSPP

Одним із істотних досягнень у сфері оптичних технологій є реконфігурувальний оптичний мультиплексор введення/виведення (Reconfigurable Optical Add/Drop Multiplexer, ROADM). Він став результатом вимог до великої прозорості та гнучкості перспективних мультисервісних конвергентних мереж на основі повністю оптичних мереж AON. Від впровадження реконфігурувальних мультиплексорів ROADM передбачається отримати такі додаткові можливості:

– з’єднання вузлів типу “будь-який з будь-яким”. Причому всі з’єднання реалізуються на оптичному рівні без використання опто-електронно-оптичного перетворення сигналів. Це стало можливим завдяки удосконаленню характеристик системи передавання, забезпеченим за рахунок долучення функції вирівнювання посилення оптичних каналів та використання селективної відносно довжини хвилі технології;

– повністю автоматичне узгодження оптичних рівнів за рахунок зазначеної вище функції вирівнювання;

– передавачі, розраховані на широкий діапазон можливих швидкостей передавання цифрових потоків і оптичні мультиплексори для об'єднання оптичних каналів з різною швидкістю передавання сигналів.

Завдяки ROADM мережні ресурси можуть виділятися динамічно, відповідно до вимог трафіку, з урахуванням різних потреб у обсягах передавання інформації в будь-який час доби. Це стимулюватиме застосування ROADM у транспортних мережах METRO. Нові конфігураційні можливості є необхідними також для того, щоб планувати транспортування на рівні CORE. Транспортна мережа CORE спочатку була набором вузлів у вигляді потужних LSR маршрутизаторів і з'єднувальних каналів різних сервісних мереж. Еволюція транспортної мережі CORE викликає необхідність реалізації для GMPLS мережі гнучкого фотонного транспортного рівня з'єднань. Тут також можна успішно застосовувати ROADM. Більш того, якщо ступінь заповнення оптичних з'єднань є високим, ROADM дає змогу передавати транзитний трафік на потрібний LSR, не завантажуючи їм проміжні LSR. Тим самим можна знизити вимоги до продуктивності маршрутизаторів і відповідні витрати.

Підсумовуючи, можна констатувати, що мультисервісну мережу з GMPLS складатимуть такі компоненти, як маршрутизатори, DWDM системи, мультиплексори ROADM і оптичні комутатори.

Контрольні питання до розділу 4

1. Опишіть сутність технології SDH.
2. Поясніть сутність технології ATM та наведіть класифікацію класів обслуговування.
3. Поясніть сутність технології GMPLS.
4. Наведіть та поясніть структуру комірки ATM.
5. Наведіть та поясніть призначення основних елементів технології MPLS.

РОЗДІЛ 5
ПРОТОКОЛИ НАЛАШТУВАННЯ ТА ПЕРЕВІРКИ ЗВ'ЯЗАНОЇ МЕРЕЖІ З РЕЗЕРВУВАННЯМ

5.1. Основні задачі адміністрування мереж та шляхи їх вирішення

5.1.1. Роль та задачі адміністратора мереж

Завдання мережного адміністрування в складній розподіленої КС:

1. Планування мережі. Незважаючи на те, що плануванням і монтажем великих мереж зазвичай займаються спеціалізовані компанії-інтегратори, адміністраторам часто доводиться планувати певні зміни в структурі мережі – додавання нових робочих місць, додавання або видалення мережних протоколів, додавання або видалення мережних служб, установка серверів, розділення мережі на сегменти і т.д. Дані роботи повинні бути ретельно сплановані, щоб нові пристрої, вузли або протоколи включалися в мережу або виключалися з неї без порушення цілісності мережі, без зниження продуктивності, без порушення інфраструктури мережних протоколів, служб і додатків.

2. Установка і настройка мережних вузлів (пристроїв активного мережного обладнання, персональних комп'ютерів, серверів, засобів комунікацій).

А саме заміну мережного адаптера в ПК з відповідними настройками комп'ютера, перенесення мережного вузла (ПК, сервера, активного обладнання) в іншу підмережу з відповідним змінами мережних параметрів вузла, додавання або заміна мережного принтера з відповідною настроюванням робочих місць.

3. Установка і настройка мережних протоколів. Дане завдання включає в себе виконання таких робіт – планування та налаштування базових мережних протоколів корпоративної мережі, тестування роботи мережних протоколів, визначення оптимальних конфігурацій протоколів.

4. Установка і настройка мережних служб. Корпоративна мережа може містити великий набір мережних служб. Коротко перерахуємо основні завдання адміністрування мережних служб:

– встановлення та налаштування служб мережної інфраструктури (служби DNS, DHCP, WINS, служби маршрутизації, віддаленого доступу та віртуальних приватних мереж);

– встановлення та налаштування служб файлів і друку, які в даний час складають значну частину всіх мережних служб;

– адміністрування служб каталогів (Novell NDS, Microsoft Active Directory), що складають основу корпоративної системи безпеки та управління доступом до мережних ресурсів;

– адміністрування служб обміну повідомленнями (системи електронної пошти);

– адміністрування служб доступу до баз даних.

5. **Пошук несправностей.** Адміністратор повинен вміти виявляти широкий спектр несправностей – від несправного мережного адаптера на робочій станції користувача до збоїв окремих інтерфейсів комутаторів і маршрутизаторів, а також неправильні настройки мережних протоколів і служб.

6. Пошук "вузьких" місць мережі та підвищення ефективності роботи мережі. У завдання мережного адміністрування входить аналіз роботи мережі і визначення найбільш вузьких місць, які потребують або заміни мережного обладнання, або модернізації робочих місць, або зміни конфігурації окремих сегментів мережі.

7. Моніторинг мережних вузлів. Моніторинг мережних вузлів включає в себе спостереження за функціонуванням мережних вузлів і коректністю виконання покладених на дані вузли функцій.

8. Моніторинг мережного трафіку. Моніторинг мережного трафіку дозволяє виявити і ліквідувати різні види проблем: високу завантаженість окремих мережних сегментів, надмірну завантаженість окремих мережних пристроїв, збої в роботі мережних адаптерів або інтерфейсів мережних пристроїв, небажану активність або атаки зловмисників (поширення вірусів, атаки хакерів і ін.).

9. Забезпечення захисту даних. Захист даних включає в себе великий набір різних завдань: резервне копіювання і відновлення даних, розробка і здійснення політики безпеки облікових записів користувачів і мережних служб (вимоги до складності паролів, частота зміни паролів), побудова захищених комунікацій (застосування протоколу IPSec, побудова віртуальних приватних мереж , захист бездротових мереж), планування, впровадження та обслуговування інфраструктури відкритих ключів (PKI).

Для зручності виконання обов'язків адміністратора мережі він (для нього) складають, як правило три види схем мережі різного рівня:

1. Схема з'єднань мережі, де відображаються комунікаційне обладнання з номерами інтерфейсів і кабельні лінії між ними (рисунок 5.1).

2. Топологія мережі, яка містить все наявне мережне обладнання мережі (з урахуванням його взаємного розташування) та лінії, що їх з'єднують (рисунок 5.2).

3. Логічна схема мережі, що відображає віртуальні локальних мережі, відображаються сегменти IP-мереж з їхніми адресами (рисунок 5.3).

5.1.2. Протоколи налаштування та перевірки зв'язаної мережі

Протокол CDP (Cisco Discovery Protocol – протокол виявлення устаткування Cisco) інструмент мережного адміністратора, оскільки він допоможе побудувати базову схему структури мережі. Незважаючи на те що цей протокол показує інформацію виключно тільки про безпосередньо підключені до цього вузла сусідні пристрої, він все ж є дуже потужним засобом налаштування мережі. Протокол працює на канальному рівні, який об'єднує фізичне середовище передачі даних нижнього рівня з протоколами

верхніх мережних рівнів, він використовується для отримання інформації про сусідні мережні облаштування корпорації Cisco. Отримувана інформація включає типи підключених пристроїв, інтерфейси маршрутизатора, до яких сусідні пристрої підключені, інтерфейси, що використовуються для створення з'єднань, а також моделі пристроїв.

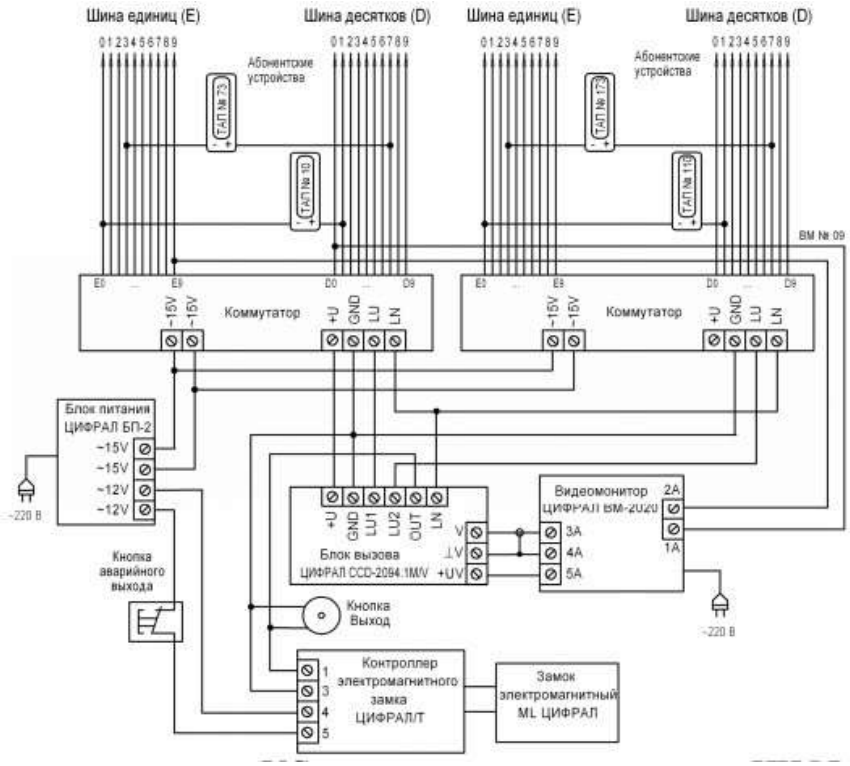


Рисунок 5.1 – Схема з'єднань мережі, де відображаються комунікаційне обладнання з номерами інтерфейсів і кабельні лінії між ними

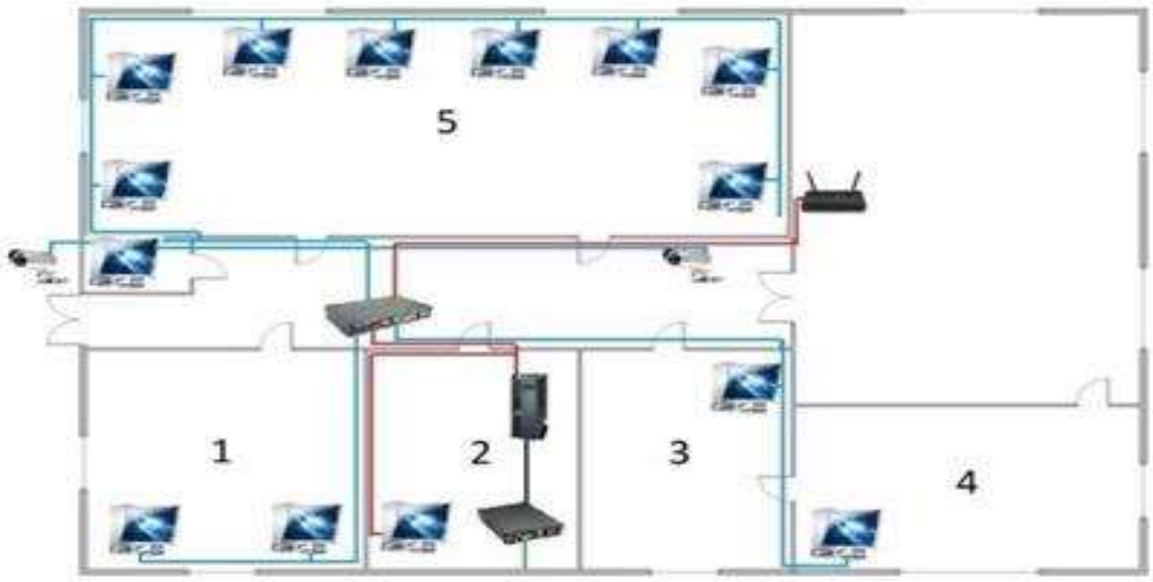


Рисунок 5.2 – Топологія мережі, яка містить все наявне мережне обладнання (з урахуванням його взаємного розташування) та лінії, що їх з'єднують

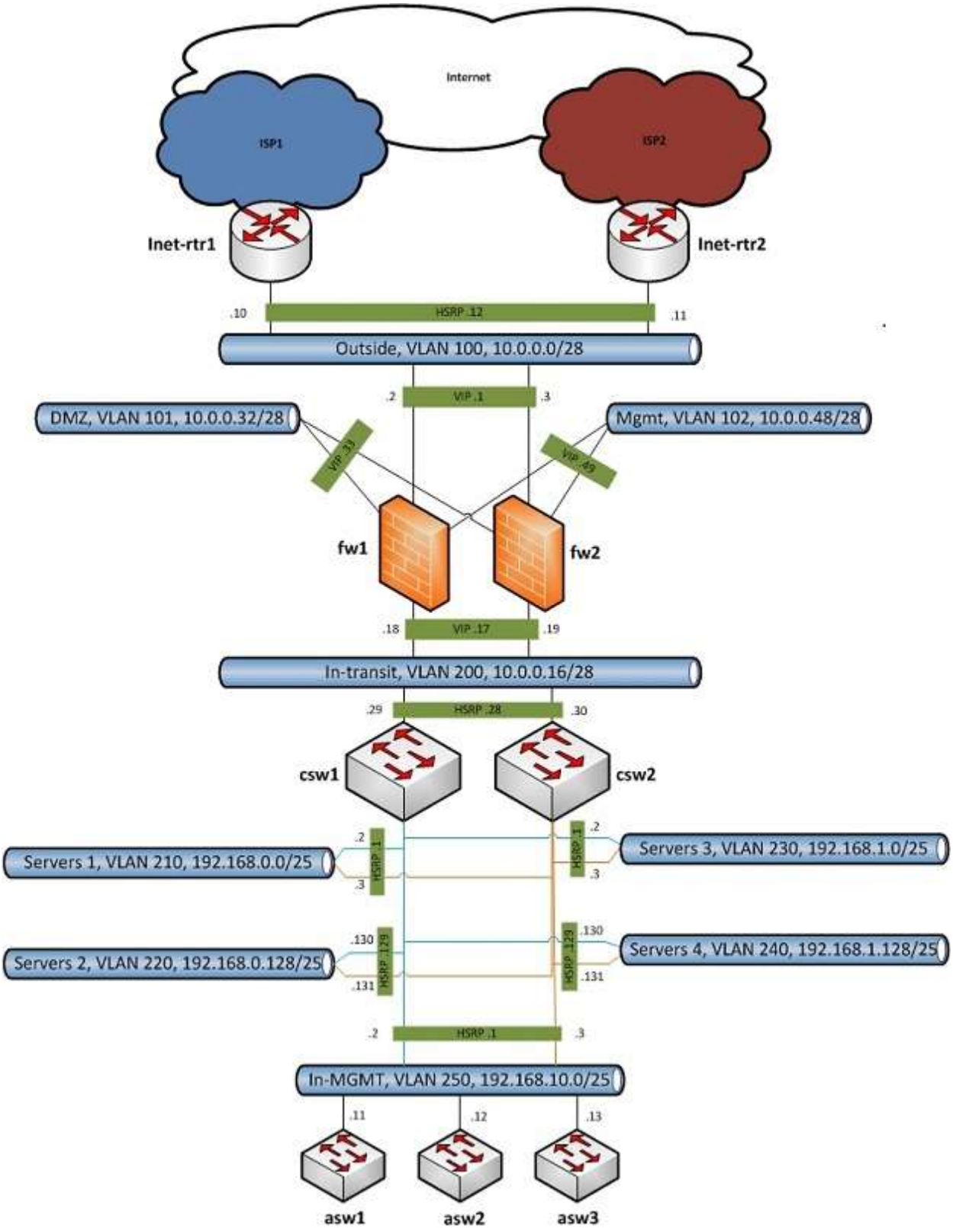


Рисунок 5.3 – Логічна схема мережі, що відображає віртуальні локальних мережі, відображаються сегменти IP-мереж з їхніми адресами

Протокол CDP не залежить від середовища передачі і від протоколів, працює з будь-яким устаткуванням корпорації Cisco і в якості своєї основи використовує протокол доступу до підмережі (SNAP – Subnetwork Access Protocol). CDP є власним протоколом мережних облаштувань Cisco і працює

тільки з мережними пристроями, випущеними компанією Cisco. Самою останньою версією протоколу CDP є версія 2 (CDPv2). Підтримка протоколу CDPv2 вже включена в операційну систему Cisco IOS Software версии12.0(3) T і пізніші.

Протокол CDP запускається автоматично при завантаженні устаткування Cisco і дозволяє мережному пристрою знаходити сусідні вузли, на яких також запущений протокол CDP.

Кожен пристрій з налагодженим протоколом CDP періодично відправляє повідомлення, також відомі як анонси (advertisement), усім сусіднім пристроям. За замовчуванням анонси розсилаються кожні 60 секунд.

Мережний пристрій, який розуміє анонси, які він періодично отримує від сусідніх пристроїв, зберігає отриману інформацію у CDP-таблиці. Якщо пристрій тричі не надіслав анонс (при значеннях за замовчуванням – 3 хвилини (180 секунд)), він видаляється з таблиці.

Основним завданням протоколу CDP є отримання даних про платформи сусідніх пристроїв і виконувані ними протоколи. CDP-фрейм може бути невеликим, проте містити масу корисної інформації про сусідні маршрутизатори і комутатори.

На рисунку 5.4 показано, як протокол CDP дозволяє адміністраторові отримати корисну інформацію про систему. Адміністратор може подивитися результати цього обміну CDP-інформацією за допомогою консолі, приєднаної до локального маршрутизатора. Для відображення інформації про мережі, безпосередньо приєднані до маршрутизатора, можна скористатися командою **show cdp neighbors**.

```
Router#show cdp neighbors
Capability Codes: R - Router, T - Trans Bridge, B - Source Route Bridge
                  S - Switch, H - Host, I - IGMP, r - Repeater, P - Phone
Device ID    Local Intrfce   Holdtme    Capability   Platform    Port ID
Switch       Fas 0/0          153            S       2960        Gig 0/1
Router       Fas 0/1          138            R       C2800       Fas 0/0
```

Рисунок 5.4 – Інформація протоколу CDP

Блоки інформації про кожен сусідній пристрій включають такі дані:

– ідентифікатор пристрою;
– номер і тип локального інтерфейсу;
– час утримання інформації;
– можливості пристрою;
– платформу;
– ідентифікатор інтерфейсу;
– доменне ім’я VTP (тільки у разі використання протоколу CDPv2);
– номер власної мережі VLAN (тільки у разі використання протоколу CDPv2);
– інформацію про наявність дуплексного з’єднання (тільки у разі використання протоколу CDPv2).

Для відображення усієї інформації, що міститься в повідомленнях використання протоколу CDP, можна використати попередню команду з додатковим ключем **show cdp meighbors detail**, як показано на рисунку 5.5.

```
Router#show cdp neighbors detail

Device ID: Switch
Entry address(es):
  IP address : 192.168.10.10
Platform: cisco 2960, Capabilities: Switch
Interface: FastEthernet0/0, Port ID (outgoing port): GigabitEthernet0/1
Holdtime: 139

Version :
Cisco IOS Software, C2960 Software (C2960-LANBASE-M), Version 12.2(25)FX, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Wed 12-Oct-05 22:05 by pt_team

advertisement version: 2
Duplex: full
---------------------------

Device ID: Router
Entry address(es):
  IP address : 11.1.1.2
Platform: cisco C2800, Capabilities: Router
Interface: FastEthernet0/1, Port ID (outgoing port): FastEthernet0/0
Holdtime: 124

Version :
Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 06:21 by pt_rel_team

advertisement version: 2
Duplex: full
```

Рисунок 5.5 – Розширена інформація протоколу CDP

Для включення протоколу CDP, отримання і відстежування CDP-інформації використовуються команди:

– **cdp run** в режимі глобальної конфігурації – включає протокол CDP в маршрутизаторі

– **cdp enable** в режим налаштування інтерфейсу – дозволяє використання протоколу CDP на інтерфейсі

– **clear cdp counters** в привілейованому режимі – скидає усі лічильники переданих даних в початковий стан.

Для відключення протоколу CDP, після того, як він був дозволений, слід використати команди **no cdp run** в режимі глобальної конфігурації або **no cdp enable** у відповідному режимі конфігурації інтерфейсу.

Аналогом протоколу CDP є ***Link Layer Discovery Protocol (LLDP)***, якій може підтримуватися на обладнанні інших виробників і виконувати схожі функції.

Telnet – це віртуальний термінальний протокол, який є частиною стека протоколів TCP/IP. Він дозволяє створювати з'єднання з видаленими вузлами, що дає можливість отримувати видалений доступ до терміналу видаленої системи. Протокол **telnet** виконується на рівні додатків моделі OSI і побудований на базі стека TCP, отже, він спрямований на коректну і послідовну доставку даних між клієнтом і сервером.

Маршрутизатор може одночасно працювати з декількома вхідними telnet з'єднаннями. Діапазон від 0 до 4 визначає п'ять віртуальних терміналів (vty) або telnet ліній. Таким чином, одночасно може бути створено до п'яти telnet сеансів.

В основному емулятор терміналу telnet використовується для з'єднання з видаленими пристроями, такими, як маршрутизатор, комутатор і сервер, для отримання інформації або їх технічного обслуговування. Цей протокол і відповідна команда є простим і універсальним засобом тестування.

Слід зазначити, що умовою для створення telnet з'єднання є наявність *встановлених паролів на line vty і на режим enable* у видаленому пристрої. Крім того, на видалених комутаторах вимагається встановити IP-адресу на Vlan і прописати default gateway. На рисунку 5.6 проілюстровані відповідні команди.

```
Switch(config)#line console 0
Switch(config-line)#password 11
Switch(config-line)#login
Switch(config-line)#end
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#enable password 11
Switch(config)#line vty 0 15
Switch(config-line)#password 11
Switch(config-line)#login
Switch(config)#interface vlan 1
Switch(config-if)#ip address 192.168.10.10 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#ip default-gateway 192.168.10.1
Switch(config)#
```

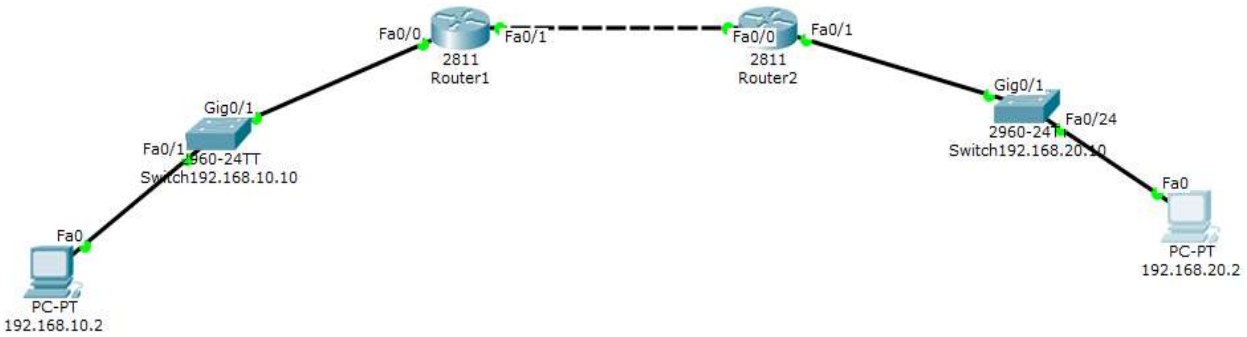
Рисунок 5.6 – Команди, що передують створенню telnet з'єднання

Для безпосереднього створення telnet з'єднання потрібно ввести в командному рядку команду **telnet** і ім'я вузла або **IP-адресу** видаленого маршрутизатора і сеанс буде ініційований. Для розриву telnet сеансу використовується команда exit або logout.

Як показано на рисунку 5.7, за допомогою telnet з'єднання користувач з комп'ютера 192.168.20.2 може встановити telnet сеанс з комутатором 192.168.10.10, який може знаходиться скільки завгодно далеко.

Протокол telnet є надзвичайно корисним, але має суттєвий недолік – обмін інформацією без її захисту (у відкритому вигляді). Це може призводити до перехоплення telnet повідомлень, що містять паролі та логіни. З метою запобігання означених прогалин безпеки рекомендоване до використання захищену версію протоколу telnet – SSH (Secure SHell – «безпечна оболонка») – мережний протокол рівня застосунків, що дозволяє

проводити віддалене управління вузлом, схожий за функціональністю з протоколом telnet, проте шифрує весь трафік, в тому числі і паролі, що передаються.




```
C:\>telnet 192.168.10.10
Trying 192.168.10.10 ...Open


User Access Verification

Password:
Switch>en
Password:
Switch#con
Switch#conf
Switch#configure ter
Switch#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#
```

Рисунок 5.7 – Процедура встановлення telnet з’єднання

Криптографічний захист протоколу SSH не фіксований, можливий вибір різних алгоритмів шифрування. Клієнти і сервери, що підтримують цей протокол, доступні для різних платформ. Для налаштування на вузлі можливості підключення за протоколом SSH, потрібно виконання низки додаткових команд (таблиця 5.1)

Таблиця 5.1 – Додаткові команди для налаштування протоколу SSH

№ з/п	Команда	Призначення
1.	cisco(config)# ip domain name test.dom	Вказуємо ім’я домену (необхідно для генерації ключа)
2.	cisco(config)# crypto key generate rsa	Генеруємо **RSA** ключ (необхідно буде вибрати розмір ключа)
3.	cisco(config)# username user privilege 15 password 7 Pa$$w0rd	Заводимо користувача з ім’ям **user**, паролем **Pa$$w0rd** і рівнем привілеїв **15**.
4.	cisco(config)# line vty 0 4 cisco(config-line)# transport input ssh	• Входимо в режим конфігурації термінальних ліній з 0 по 4. • Вказуємо середовищем доступу через мережу за замовчуванням SSH.

Для виявлення помилок при передачі мережний рівень моделі OSI використовує протокол управляючих повідомлень в мережі Internet (**Internet Control Message Protocol, ICMP**). Протокол ICMP повідомляє відправникові дані про те, що при їх доставці сталася помилка.

Знання повідомлень про помилки протоколу ICMP і потенційних причин появи таких повідомлень є суттєвою частиною процесу пошуку і усунення помилок в мережах. Протокол ICMP є одним з компонентів стека TCP/IP (Transmission Control Protocol / Internet Protocol протокол управління передачею/протокол мережі Internet), який компенсує нездатність протоколу IP гарантовано доставляти дані.

В той же час протокол ICMP не усуває ненадійність передачі даних протоколом IP. Він лише повідомляє відправника даних про те, що при їх доставці виникли проблеми. Протокол ICMP є механізмом відправки повідомлень про помилки для протоколу IP. Якщо при доставці дейтаграми відбувається помилка, протокол ICMP повідомляє про це відправника дейтаграми. Наприклад, припустимо, що робоча станція 1, показана на рисунку 5.8, посилає дейтаграму робочої станції 6.

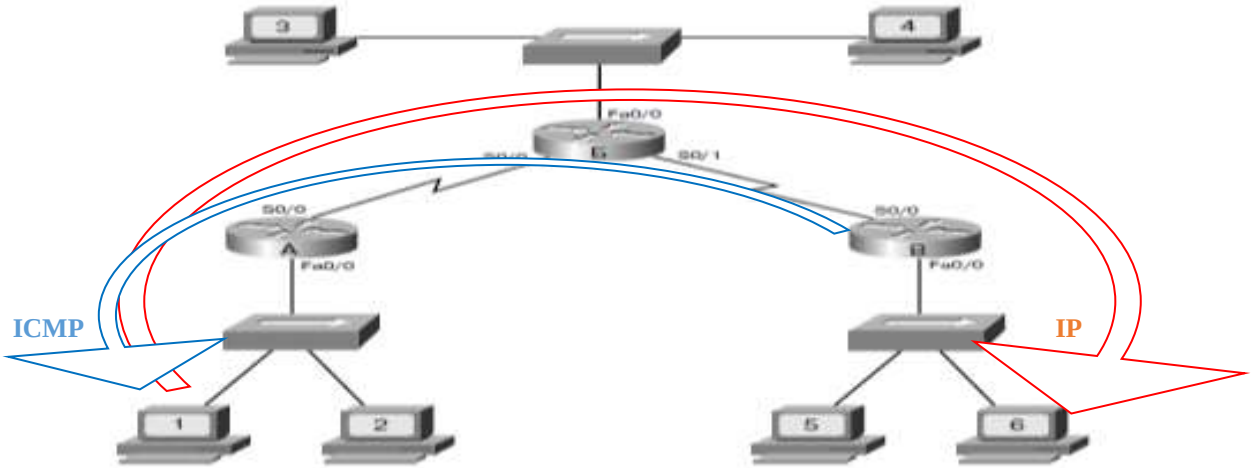


Рисунок 5.8 – Робота протоколу ICMP

Якщо відповідний інтерфейс маршрутизатора B виходить з ладу, цей маршрутизатор використовує протокол ICMP для відправки робочої станції 1 повідомлення про те, що доставка дейтаграми виявилася неможливою. Протокол ICMP не усуває проблему, що виникла в мережі. Усе, що може зробити протокол ICMP, це відправити робочій станції 1 повідомлення про помилку.

Можливість здійснення зв'язку через мережу залежить від описаних нижче трьох основних умов. У станції-відправника і одержувачі має бути правильно зконфігурований стек протоколів TCP/IP. Ця вимога включає установку засобів стека протоколів TCP/IP і відповідну конфігурацію IP-адреси і маски підмережі.

Якщо передбачається відправка дейтаграм за межі локальної мережі, то має бути зконфігурований і стандартний шлюз.

Для передачі дейтаграми від пристрою-відправника, що знаходиться в одній мережі, в мережу одержувача через інші мережі в останніх мають бути присутніми відповідні проміжні пристрої. Цю функцію виконують маршрутизатори.

На інтерфейсах маршрутизатора мають бути правильно зконфігуровані протокол TCP/IP і протокол маршрутизації або статичні маршрути.

Якщо перелічені вище умови не виконані, то здійснення зв'язку неможливе. Наприклад, відправник може послати дейтаграму на неіснуючу IP-адресу або пристрою-одержувачеві, який від'єднаний від мережі. Причиною неможливості доставки може стати також маршрутизатор, якщо відповідний його інтерфейс вийшов з ладу або він не має інформації, необхідної для знаходження мережі-одержувача. У такому разі недоступна мережа одержувача називається недосяжною мережею (unreachable network). Повідомлення про недосяжність пункту призначення можуть включати наступні види інформації:

– *мережа недосяжна* – це повідомлення зазвичай свідчить про помилки в маршрутизації або адресації;

– *вузол недосяжний* – це повідомлення зазвичай свідчить про помилки при доставці, наприклад, про помилкову маску підмережі;

– *протокол недоступний (недосяжний)* – це повідомлення зазвичай свідчить про те, що пункт призначення не підтримує протокол верхнього рівня, вказаний в пакеті;

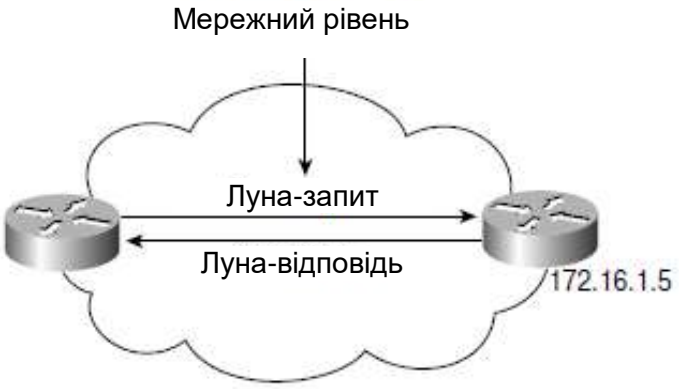
– *порт недосяжний* – це повідомлення зазвичай свідчить про те, що TCP-порт (сокет) недоступний.

Утиліта ping. Більшість мережних пристроїв підтримують луна-утиліту **ping**, яка використовує протокол ICMP і дозволяє провести просту перевірку мережного з'єднання. Луна-утиліта дозволяє перевірити коректність маршрутизації мережних пакетів. Команда ping відправляє пакети одержувачеві і потім чекає пакетів у відповідь від цього вузла. Результати роботи такої луна-утиліти можуть допомогти оцінити надійність з'єднання, затримки передачі пакетів, а також працездатність вузла. Команда ping є основним механізмом тестування з'єднання і може бути викликана з призначеного для користувача або привілейованого режиму.

Для перевірки з'єднання за допомогою команди ping слід виконати дії: Ввести команду **ping [IP-address]** чи **[name]** одержувача і натиснути клавішу <Enter>. На рисунку 5.9 приведена діаграма мережі, що ілюструє процес роботи служби відправки луна-запитів і прийому відповідей.

Утиліта traceroute. Утиліта traceroute (також для вузлів Windows використовується її варіант tracert) є відмінним інструментом, який дозволяє відстежити відправника і маршрут проходження потоку даних по мережі. Утиліта traceroute схожа на утиліту ping, проте дозволяє відстежити не лише стан кінцевих точок маршруту, але і стан кожного транзитного переходу пакетів в мережі. Ця команда може бути виконана як з призначеного для користувача, так і з привілейованого режиму. Команда traceroute

використовується таким чином: Ввести команду **traceroute [IP-address]** чи**[name] (ім'я)** одержувача і натиснути клавішу <Enter> (рисунок 5.10).




```
C:\>ping 192.168.10.2

Pinging 192.168.10.2 with 32 bytes of data:

Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time=1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126
Reply from 192.168.10.2: bytes=32 time<1ms TTL=126

Ping statistics for 192.168.10.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms
```

Рисунок 5.9 – Робота утиліти ping

```
C:\>tracert 192.168.10.2

Tracing route to 192.168.10.2 over a maximum of 30 hops:

  1    0 ms      0 ms      0 ms      192.168.20.1
  2    0 ms      0 ms      0 ms      11.1.1.1
  3    0 ms      1 ms      0 ms      192.168.10.2

Trace complete.
```

Рисунок 5.10 – Робота утиліти traceroute

Утиліта traceroute використовує повідомлення про помилки, генеровані маршрутизаторами, коли витікає час життя пакету (TTL) або перевищується значення максимального числа переходів. Команда traceroute відправляє декілька ping-пакетів зі значенням TTL, що збільшується, і відображає час їх проходження. Оскільки кожен пакет, що послідовно відправляється, має менший час життя, то кожен подальший знищується на ближчій ділянці мережі. Одним із застосувань команди traceroute є пошук несправної ділянки мережі.

5.2. Протокол взаємодії мереж 2 рівня stp

5.2.1. Побудова та недоліки топології на комутаторах з резервними каналами зв'язку

Резервування є важливою частиною ієрархічної конструкції й запобігає виникненню перебоїв в наданні сервісів користувачам. Для резервування потрібне додавання надмірних фізичних шляхів, а також логічне резервування.

Трирівнева ієрархічна модель мережі (рисунок 5.11), яка містить ядро, рівні розподілу і доступу з надлишковістю, дозволяє усунути точку відмови в мережі за рахунок альтернативних фізичних каналів для передачі даних по мережі.

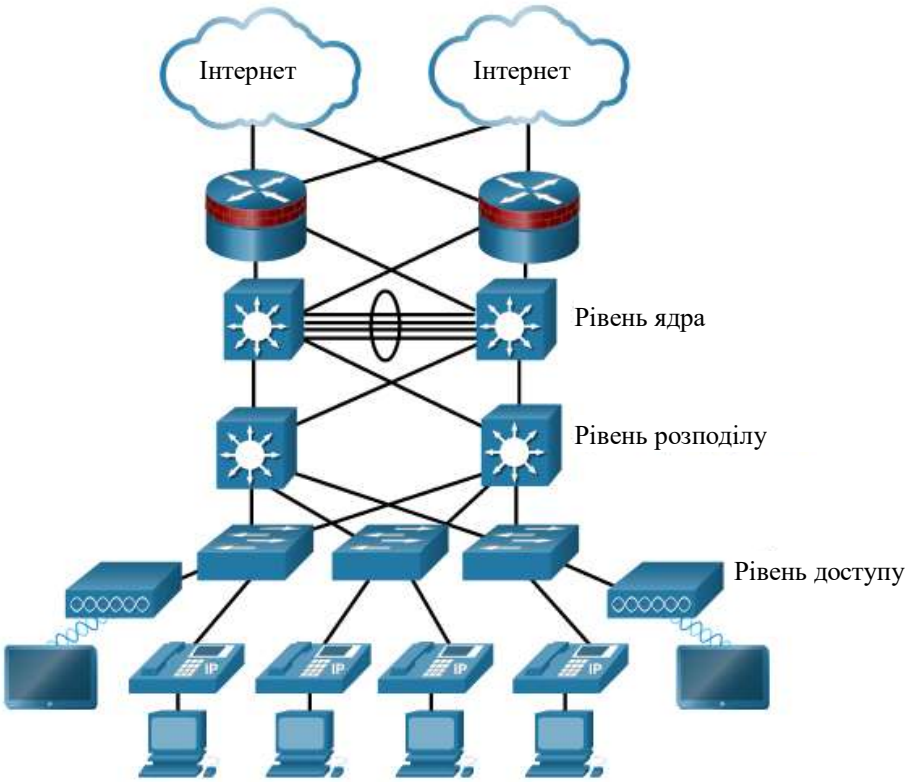


Рисунок 5.11 – Ієрархічна модель трьохрівневої мережі

В комутованій мережі (рисунок 5.12) наявність надлишковості дозволяє створювати альтернативні шляхи передачі інформації:

– PC1 взаємодіє з PC4 через надлишкову топологію мережі, використовуючи Магістраль 1.

– При розриві мережного каналу між комутаторами S1 і S2 шлях між комп'ютерами PC1 і PC4 автоматично коригується певним протоколом для компенсації цього розриву.

– При відновленні мережного з'єднання між S1 і S2 цей шлях коригується протоколом заново, і трафік на PC4 направляється безпосередньо від S2 до S1.

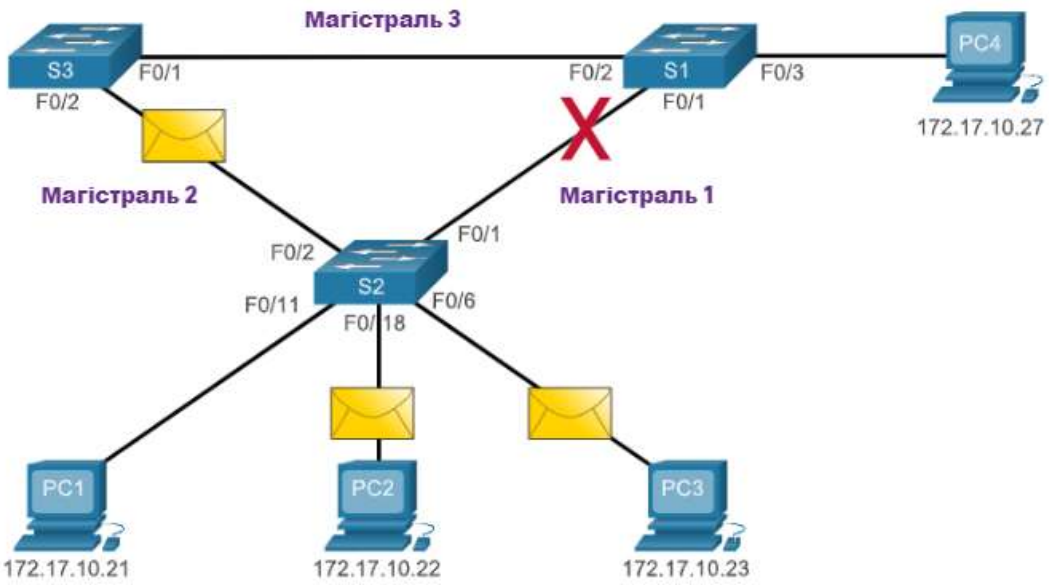


Рисунок 5.12 – Мережа з надлишковістю

Внаслідок роботи комутаторів, особливо в процесі отримання даних і пересилання, можуть виникати логічні петлі 2-го рівня. При наявності декількох шляхів між двома пристроями та відсутності реалізації протоколу spanning-tree виникає петля 2-го рівня. Петля 2-го рівня може призвести до трьох основних проблем, а саме:

Нестабільність бази даних MAC-адрес

У кадрів Ethernet немає атрибута “термін життя” (TTL). Як результат, якщо не використовується механізм блокування постійного поширення цих кадрів в комутованій мережі, кадри продовжують поширюватися між комутаторами нескінченно або до тих пір, поки не відбудеться збій каналу, в результаті чого петля буде перервана. Таке постійне поширення між комутаторами може привести до нестабільності бази даних MAC-адрес. Це може статися внаслідок пересилання широкомовних кадрів.

Широкомовні кадри пересилаються з усіх інтерфейсів комутатора, за винятком вихідного вхідного інтерфейсу. Це гарантує, що всі пристрої в домені широкомовної розсилки можуть отримати кадр. При наявності більш одного шляху, з якого пересилається кадр, може виникнути нескінченна петля. При появі петлі виникає можливість постійної зміни таблиці MAC-адрес на комутаторі оновленнями з кадрів широкомовної розсилки, що призводить до нестабільності бази даних MAC-адрес:

– Комп’ютер PC1 відправляє широкомовний кадр на S2. S2 приймає широкомовний кадр на інтерфейс F0/11. Коли S2 приймає широкомовний кадр, він оновлює свою таблицю MAC-адрес, щоб зареєструвати доступність PC1 на інтерфейсі F0/11.

– Оскільки цей кадр широкомовний, S2 пересилає кадр з усіх інтерфейсів, включаючи Магістраль 1 і Магістраль 2. При надходженні кадру широкомовної розсилки на комутатори S3 і S1 ці комутатори оновлюють свої таблиці MAC-адрес, вказуючи, що комп’ютер PC1 доступний з інтерфейсу F0/1 комутатора S1 і з інтерфейсу F0/2 комутатора S3.

– Оскільки цей кадр є широкомовним, S3 і S1 пересилають кадр з усіх інтерфейсів, за винятком вихідного вхідного інтерфейсу. S3 відправляє широкомовний кадр з PC1 на S1. S1 відправляє широкомовний кадр з PC1 на S3. Всі комутатори оновлюють свою таблицю MAC-адрес з урахуванням неправильного інтерфейсу PC1.

– Кожен комутатор пересилає кадр широкомовної розсилки з усіх своїх інтерфейсів, за винятком вхідного інтерфейсу, внаслідок чого обидва комутатора пересилають кадр на комутатор S2.

– При отриманні комутатором S2 кадрів широкомовної розсилки з S3 і S1 таблиця MAC-адрес оновлюється останнім записом, отриманої з інших двох комутаторів.

Цей процес повторюється кожного разу заново доти, поки петля не буде розірвана фізичним розривом її сполук або вимиканням живлення одного з комутаторів у петлі. При цьому створюється високе навантаження на центральні процесори (ЦП) на всіх комутаторах, що беруть участь в петлі. Оскільки між усіма комутаторами в петлі постійно передаються одні і ті ж кадри, ЦП комутатора доводиться обробляти великий обсяг даних. При цьому знижується продуктивність комутатора при надходженні допустимого трафіку.

Вузол, який бере участь в мережній петлі, недоступний для інших вузлів в мережі. Крім того, внаслідок постійних змін в таблиці MAC-адрес комутатор не знає, з якого інтерфейсу слід пересилати кадри одноадресної розсилки. У вищевказаному прикладі для PC1 перераховані неправильні інтерфейси. Будь-якій одноадресний кадр, призначений для PC1, пересилається в мережі по петлі, подібно широкомовною кадрам. Через зростаючу кількість кадрів, які формують петлю в мережі, в кінцевому підсумку утворюється широкомовний шторм.

Широкомовний шторм

Широкомовний шторм виникає в разі, коли в петлю на другому рівні потрапляє стільки кадрів широкомовної розсилки, що при цьому споживається вся доступна смуга пропускання. Відповідно, для легітимного трафіку немає доступної смуги пропускання, і мережа стає недоступною для обміну даними. Це призводить до відмови в обслуговуванні (DoS).

Широкомовний шторм (рисунок 5.13) неминучий в мережі, де виникла петля. Чим більше пристроїв відправляє широкомовне розсилання по мережі, тим більше трафіку потрапляє в цикл і споживає ресурси. В кінцевому рахунку це створює широкомовний шторм, що призводить до збоїв в мережі:

– PC1 передає кадр широкомовної розсилки в мережу, де виникла петля.

– Кадр широкомовної розсилки циклічно передається між усіма з’єднаними між собою комутаторами в мережі.

– PC4 також передає кадр широкомовної розсилки в мережу, де виникла петля.

– Кадр широкомовної розсилки PC4 потрапляє в петлю між усіма взаємно з'єднаними комутаторами, подібно кадру широкомовної розсилки PC1.

– Чим більше пристроїв відправляє широкомовне розсилання по мережі, тим більше трафіку потрапляє в цикл і споживає ресурси. В кінцевому рахунку це створює широкомовний шторм, що призводить до збоїв в мережі.

– Коли мережу повністю насичена трафіком широкомовної розсилки, який циклічно передається між комутаторами, новий трафік відкидається комутатором, оскільки він не в змозі його обробити.

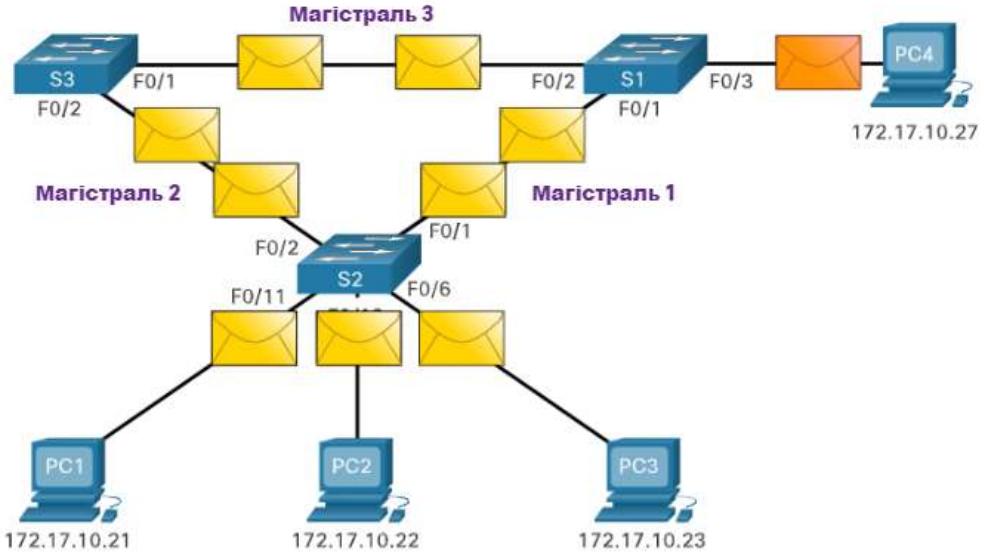


Рисунок 5.13 – Широкомовний шторм

Широкомовні шторми також мають і ряд інших наслідків. Оскільки широкомовний трафік пересилається з кожного інтерфейсу на комутаторі, всім підключеним до нього пристроям необхідно обробляти весь цей широкомовний трафік, обсяг якого в мережу з петлею весь час зростає. Це може викликати порушення функціонування кінцевого пристрою, якщо воно не зможе обробляти таке велике навантаження трафіку на своїй мережній інтерфейсній платі (NIC).

Широкомовний шторм може виникнути за кілька секунд, так як підключення до мережі пристрою регулярно відправляють кадри широкомовної розсилки, наприклад запити ARP. В результаті при виникненні петлі коммутируемая мережу швидко виходить з ладу.

Дубльовані одноадресні кадри

Кадри широкомовної розсилки є не єдиним типом кадрів, на які впливає виникнення петель. Невідомі одноадресні кадри, відправлені в циклічну мережу, можуть призводити до появи дубльованих кадрів, що надходять на цільовий пристрій. Невідомий одноадресний кадр з комутатора формується, коли у комутатора немає MAC-адреси призначення в таблиці

MAC-адрес, і він повинен переслати цей кадр зі всіх своїх інтерфейсів, за винятком вхідного інтерфейсу:

– PC1 відправляє кадр одноадресної розсилки, призначений для PC4.

– У таблиці MAC-адрес на комутаторі S2 немає запису PC4. У спробі знайти PC4 він розсилає невідомий одноадресний кадр з усіх своїх інтерфейсів, за винятком інтерфейсу, який прийняв цей трафік.

– Кадр надходить на комутатори S1 і S3.

– На комутаторі S1 є запис MAC-адреси PC4, тому він пересилає кадр на PC4.

– На комутаторі S3 є запис PC4 в таблиці MAC-адрес, тому він пересилає одноадресний кадр з інтерфейсу Trunk3 на S1.

– S1 приймає дубльований кадр і відправляє його на PC4.

– Таким чином, PC4 приймає два однакових кадри.

Більшість протоколів верхнього рівня не призначені для розпізнавання дубльованих передач. Як правило, протоколи, що використовують механізм нумерації послідовності, припускають, що стався збій передачі, і номер послідовності переходить в інший сеанс обміну даними. Інші протоколи намагаються перекласти дубльовану передачу на відповідний протокол верхнього рівня для обробки з можливим відхиленням.

Протоколи LAN 2-го рівня, наприклад Ethernet, не включають в себе механізм для розпізнавання і видалення нескінченних петльових кадрів. Деякі протоколи 3-го рівня використовують механізми часу життя (TTL), які обмежують кількість спроб повторної передачі пакетів мережними пристроями 3-го рівня. Пристрої 2-го рівня не володіють таким механізмом, тому продовжують повторно передавати петльовий трафік необмежено довго. Для вирішення таких проблем був розроблений **STP** (Spanning Tree Protocol) – механізм запобігання петель 2-го рівня.

Щоб уникнути подібних проблем в мережі з надмірністю, на комутаторах повинні бути включені певні типи протоколу spanning-tree. Протокол spanning-tree за замовчуванням включений на комутаторах Cisco, запобігаючи, таким чином, виникненню петель 2-го рівня.

Щоб уникнути виникнення петель 2-го рівня потрібно керувати кількома маршрутами. Вибираються оптимальні маршрути, і альтернативний маршрут повинен бути негайно доступний в разі збою основного маршруту. Протокол STP використовується для створення єдиного шляху через мережу 2-го рівня.

Термін Spanning Tree Protocol (протокол spanning-tree) і абревіатура STP відповідають протоколу 802.1D. У новітній документації IEEE по протоколу сполучного дерева (IEEE-802-1D-2004) зазначено: «STP тепер замінений протоколом Rapid Spanning Tree Protocol (RSTP)».

5.2.2. Призначення та логіка роботи протоколу STP

Протокол STP забезпечує наявність тільки одного логічного шляху між усіма вузлами призначення в мережі шляхом навмисного блокування резервних шляхів, які могли б викликати петлю.

Порт вважається заблокованим (рисунок 5.14), коли заблокована відправка і прийом даних на цей інтерфейс. До таких даних не належать кадри BPDU, які використовуються протоколом STP для запобігання петель. Для запобігання петель в мережі надзвичайно важливо блокувати надлишкові шляхи. Фізичні шляхи як і раніше використовуються для забезпечення надлишковості, однак ці шляхи відключені з метою запобігання петель. Якщо буде необхідно компенсувати несправність мережного кабелю або комутатора, протокол STP повторно розраховує шляхи і знімає блокування з певних інтерфейсів, щоб дозволити активацію надлишкового шляху.

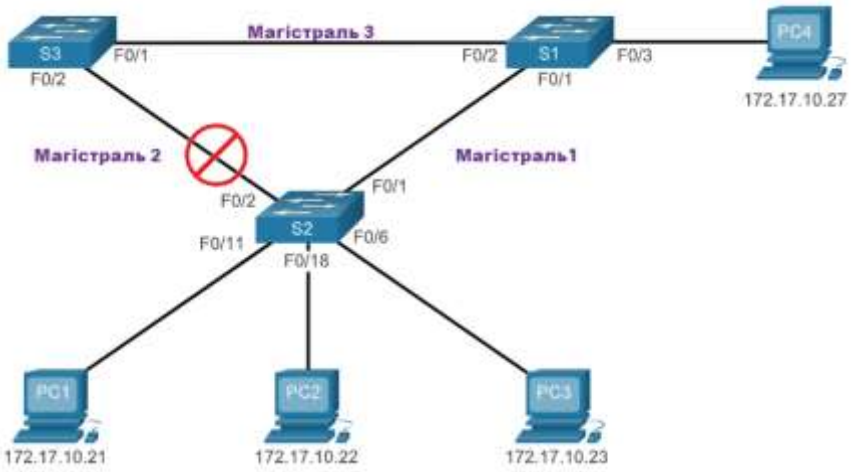


Рисунок 5.14 – Логіка роботи протоколу STP

У розглянутому прикладі протокол STP включений на всіх комутаторах:

– PC1 відправляє широкомовне розсилання в мережу.

– S2 налаштований з використанням протоколу STP, і для інтерфейсу F0/2 задано стан блокування. Стан блокування не дозволяє інтерфейсам пересилати призначені для користувача дані, що запобігає виникненню петлі. S2 пересилає кадр широкомовної розсилки з усіх інтерфейсів комутатора, за винятком інтерфейсу джерела – PC1 і інтерфейсу F0/2.

– S1 приймає кадр широкомовної розсилки і пересилає його з усіх інтерфейсів комутатора крім того, звідки він надходить, тобто до PC4 і S3. S3 пересилає кадр з інтерфейсу F0/2, але S2 не пропускає цей кадр. Виникнення петлі 2-го рівня попереджено.

Ролі інтерфейсів

У протоколах IEEE 802.1D STP і RSTP для визначення інтерфейсів комутатора в мережі, які повинні бути переведені в стан блокування для запобігання виникненню петель, використовується алгоритм протоколу

сполучного дерева (STA). STA призначає один з комутаторів як кореневий міст і використовує його в якості точки прив'язки для розрахунку всіх шляхів.

Визначивши найкращі шляхи до кореневого мосту для кожного комутатора, алгоритм STA призначає ролі інтерфейсам комутаторів. Ролі інтерфейсів описують їх зв'язок з кореневим мостом в мережі, а також вказують, чи дозволено для них пересилання трафіку:

– ***Кореневі інтерфейси*** – інтерфейси комутатора, найближчі до кореневого мосту з точки зору загальної вартості маршруту до нього. На рисунку 5.14 кореневим інтерфейсом, обраним STP на S2, буде F0/1 – канал між S2 і S1. Кореневим інтерфейсом, обраним STP на S3, буде F0/1 – канал між S3 і S1. Кореневі інтерфейси вибираються для кожного комутатора окремо.

– ***Призначені інтерфейси*** – все некореневі інтерфейси, яким, проте, дозволено пересилати трафік по мережі. На рисунку 5.14 інтерфейси комутатора S1 (F0/1 і F0/2) є призначеними інтерфейсами. На комутаторі S2 інтерфейс F0/2 також налаштований як призначений інтерфейс. Призначені інтерфейси вибираються для кожного сегмента на основі вартості кожного інтерфейсу з обох сторін сегмента та сукупну вартість, обчисленої протоколом STP для маршруту від цього інтерфейсу до кореневого мосту. Якщо на одному кінці сегмента знаходиться кореневий інтерфейс, на іншому кінці буде призначений інтерфейс. Всі інтерфейси на кореневому мосту є призначеними інтерфейсами.

– ***Альтернативні і резервні інтерфейси*** – знаходяться в стані відхилення або блокування для запобігання петель. На рисунку 5.14 STA налаштував порт F0/2 на комутаторі S3 в ролі альтернативного інтерфейсу. Цей інтерфейс на комутаторі S3 знаходиться в стані блокування. Альтернативні інтерфейси вибираються тільки на каналах, де ні з одного з кінців не має кореневого інтерфейсу. Зверніть увагу, що на рисунку заблокований тільки один кінець сегмента, це дозволяє при необхідності швидше перейти в стан пересилки.

– ***Відключені інтерфейси*** – відключеним називається комутаційний інтерфейс, живлення якого відключено.

Кореневий міст

Як показано на рисунку 5.15, протокол spanning-tree для кожної комутованої мережі LAN або кожного домену широкомовного розсилання визначає комутатор, який виконує функцію кореневого моста. Кореневий міст служить точкою прив'язки для всіх розрахунків протоколу spanning-tree, дозволяючи визначити надлишкові шляхи, які слід заблокувати.

На рисунку 5.15 кореневий міст (комутатор S1) обраний за допомогою спеціального процесу вибору. Всі комутатори, які беруть участь в STP, обмінюються кадрами BPDU для визначення комутатора з найменшим ідентифікатором моста (BID) в мережі. Комутатор з найменшим значенням BID автоматично стає кореневим мостом для розрахунків STA.

На рисунку 5.16 показані поля BID. Ідентифікатор BID складається з значення *пріоритету, розширеного ідентифікатора системи і MAC-адреси комутатора*.

Пріоритет моста являє собою значення, яке можна використовувати для визначення комутатора, що стане кореневим мостом. Комутатор з найнижчим пріоритетом, який має найменше значення BID, стає кореневим мостом. Наприклад, щоб призначити в якості кореневого моста конкретний комутатор, то для нього слід задати більш низьке значення пріоритету, ніж для інших комутаторів в мережі. Значення пріоритету за замовчуванням для всіх комутаторів Cisco дорівнює значенню 32768. Значення варіюються в діапазоні від 0 до 61440 з кроком в 4096. Допустимі значення пріоритету: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 і 61440. Всі інші значення відхиляються. Пріоритет моста 0 має перевагу в порівнянні з усіма іншими значеннями.

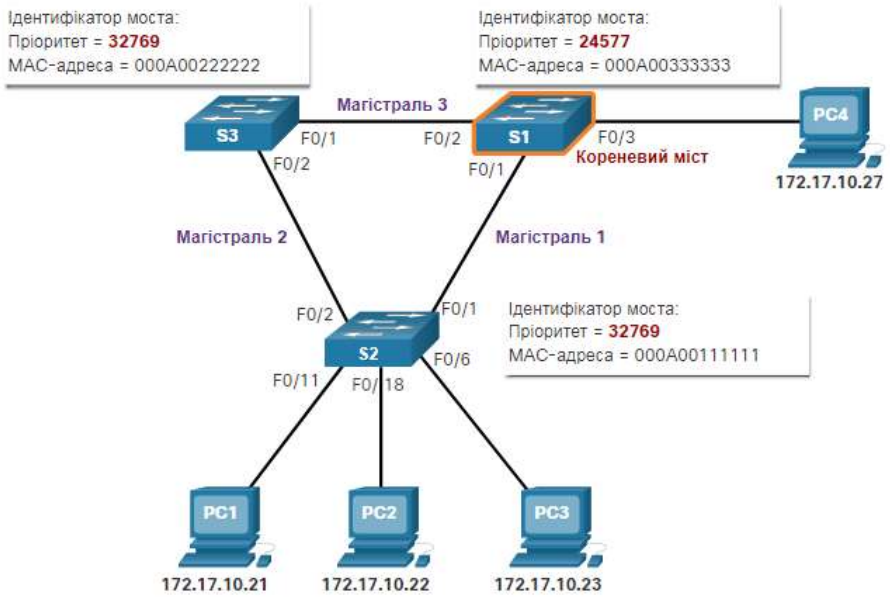


Рисунок 5.15 – Визначення кореневого мосту

Рисунок 5.16 – Ідентифікатор моста (BID)

Відомості про мережу VLAN включені в кадр BPDU за допомогою ***розширеного ідентифікатора системи***. Як показано на рисунку 5.16, в ідентифікаторі моста після 4 бітів пріоритету моста, розміщені 12 бітів – для розширеного ідентифікатора системи, який дорівнює номеру мережі VLAN, що бере участь в конкретному процесі STP. Отже, оскільки крайні праві 12 бітів резервуються для ідентифікатора мережі VLAN, а крайні ліві 4 біти –

для пріоритету моста, стає зрозумілим чому значення пріоритету моста можна налаштувати тільки кратним 4096 або 2^{12}. Якщо крайні ліві біти будуть рівні 0001, то пріоритет моста має значення 4096. Якщо крайні ліві біти рівні 1111, пріоритет моста має значення 61440 (= 15 × 4096).

Всі комутатори в домені широкомовної розсилки беруть участь в процесі вибору. Після завантаження комутатора вони починають розсилати кадри BPDU *з інтервалом у дві секунди*. **BPDU** – це кадр повідомлень протоколу STP (рисунок 5.17), яким обмінюються комутатори для забезпечення роботи даного протоколу.

Кадр BPDU містить 12 спеціальних полів, що містять інформацію про шляхи і пріоритеті, що використовується для визначення кореневого моста і шляхів до нього.

– У перших чотирьох полях вказані протокол, версія, тип повідомлення і прапори стану.

– Наступні два поля служать для ідентифікації комутатора, якого відправник кадру вважає кореневим мостом і вартості шляху до нього від відправника.

– Далі два поля, що ідентифікують сам комутатор-відправник та його інтерфейс, через який відбулась відправка кадру.

– Останні чотири поля все є полями таймерів, що визначають частоту відправлення повідомлень BPDU і тривалість зберігання інформації, отриманої через процес BPDU.

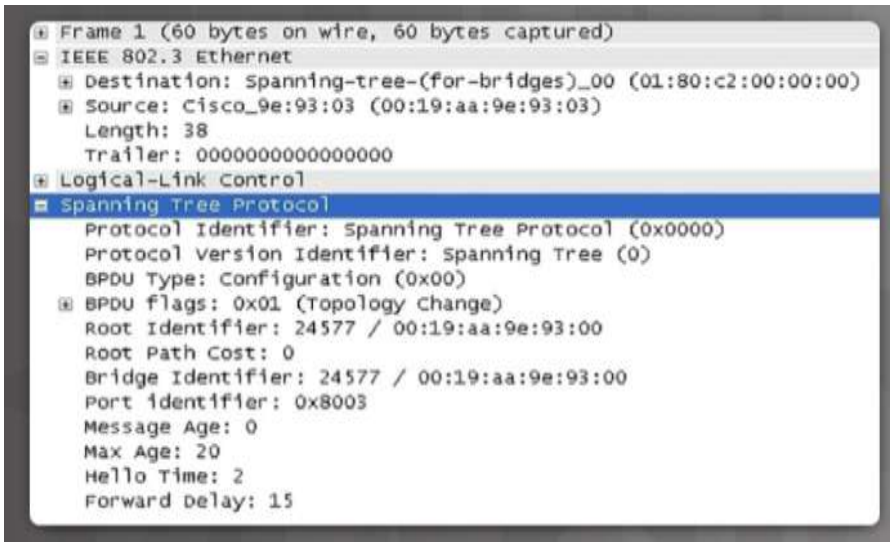


Рисунок 5.17 – Приклад кадру BPDU

На рисунку 5.17 показаний кадр BPDU, отриманий за допомогою програми Wireshark. У цьому прикладі кадр BPDU містить більшу кількість полів, ніж описано вище. Повідомлення BPDU при передачі по мережі інкапсулюється в кадр Ethernet, де в заголовку вказуються адреси джерела і призначення кадру BPDU. Кадр на рисунку містить MAC-адресу призначення 01:80:C2:00:00:00, яка є адресою групової розсилки для групи протоколу spanning-tree. Коли адресується кадр з цим MAC-адресою, кожен

комутатор, на якому налаштований протокол сполучного дерева, приймає і зчитує інформацію з кадру. Всі інші пристрої в мережі нехтують цим кадром.

Кожен комутатор в домені широкомовної розсилки спочатку передбачає, що він є кореневим мостом. Надалі комутатори пересилають свої кадри BPDU, а суміжні комутатори в домені широкомовної розсилки зчитують з них дані про ідентифікатор кореневого моста відправника. Якщо ідентифікатор кореневого моста отриманого кадру BPDU має менше значення, ніж ідентифікатор кореневого моста на приймаючому комутаторі, то в цьому випадку комутатор-приймач оновлює свій ідентифікатор кореневого моста, вказуючи в якості кореневого моста комутатор, зазначений в кадрі BPDU. Цей комутатор не обов'язково розташований поблизу, це може бути будь-який інший комутатор в домені широкомовної розсилки. Потім комутатор пересилає нові кадри BPDU з меншим значенням ідентифікатора кореневого моста на інші суміжні комутатори. Поступово комутатор з найменшим значенням ідентифікатора BID визначається як кореневий міст для протоколу spanning-tree певного домену широкомовної розсилки.

На рисунку 5.15 комутатор S1 має більш низьке значення пріоритету, ніж інші комутатори. Тому він є кращим кореневим мостом для даного екземпляра протоколу сполучного дерева.

Якщо все комутатори налаштовані з однаковим пріоритетом, як у випадку, коли всі комутатори зберігають конфігурацію за замовчуванням з пріоритетом 32768 – MAC-адреса стає визначальним фактором в тому, який комутатор стане кореневим мостом, як показано на рисунку 5.18.

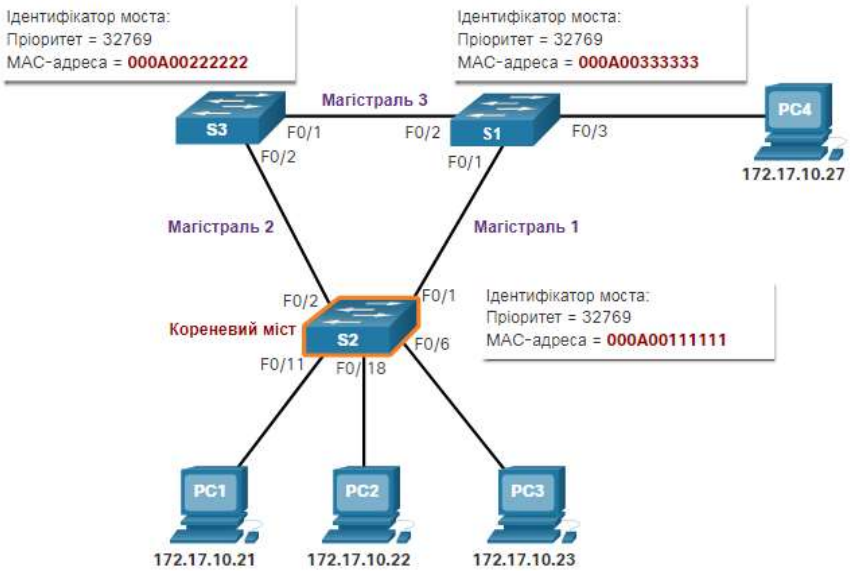


Рисунок 5.18 – Визначення кореневого мосту за MAC-адресою

У цьому прикладі для всіх комутаторів використовується значення 32769. Це значення засноване на значенні пріоритету за умовчанням 32768 і номері мережі VLAN 1, що застосована в кожному з комутаторів (32768 + 1). В такому випадку, комутатор з найнижчим шістнадцятковим значенням MAC-адреси вважається кращим кореневих мостом. У цьому прикладі S2 має

найменше значення MAC-адреси і буде призначений кореневим мостом для протоколу spanning-tree цього домену.

Кореневий міст вибирається для кожного екземпляра протоколу spanning-tree. Можлива наявність декількох окремих кореневих мостів для різних наборів мереж VLAN. Якщо всі порти на всіх комутаторах є учасниками мережі VLAN 1, значить, існує тільки один екземпляр протоколу spanning-tree. Розширений ідентифікатор системи включає в себе ідентифікатор мережі VLAN і бере участь в тому, як визначаються примірники протоколу сполучного дерева.

Після визначення кореневого моста для примірника протоколу spanning-tree, STA починає процес визначення *оптимальних шляхів до кореневого мосту* від всіх некореневих комутаторів в домені широкомовної розсилки.

Отримані алгоритмом STA значення вартості шляхів використовуються для визначення інтерфейсів, що підлягають блокуванню. Поки STA визначає оптимальні шляхи до кореневого моста для всіх інтерфейсів комутаторів мережі пересилання трафіку у цьому домені широкомовної розсилки заблоковане.

Інформацію про вартість шляху до кореневого мосту називають вартістю внутрішнього кореневого шляху. Вона дорівнює сумі вартості окремих портів на шляху від даного комутатора до кореневого мосту.

Комутатори відправляють повідомлення BPDU, які включають в себе вартість кореневого шляху. Це вартість шляху від комутатора-відправника до кореневого мосту. Коли комутатор отримує блок BPDU, він додає вартість свого вхідного порту до отриманого значення для визначення своєї вартості для внутрішнього кореневого шляху. Якщо для вибору є кілька шляхів, то шляхи з найменшою вартістю стають кращими, а всі інші надлишкові шляху блокуються.

Вартість портів за замовчуванням визначається швидкістю роботи порту, стандартні значення наведені в таблиці 5.2.

Таблиця 5.2 – Стандартні значення вартості портів для STP

Швидкість каналу	**Вартість STP, IEEE 802.1D-1998**	**Вартість RSTP, IEEE 802.1W-2004**
10 Гбіт/с	2	2000
1 Гбіт/с	4	20 000
100 Мбіт/с	19	200 000
10 Мбіт/с	100	2 000 000

Хоча з портами комутатора пов’язано значення вартості шляху за замовчуванням, значення вартості порту можна налаштувати. Можливість настройки окремих портів надає адміністратору необхідну гнучкість при контролі шляхів протоколу spanning-tree до кореневого мосту.

Щоб налаштувати вартість порту інтерфейсу, треба ввести команду *spanning-tree cost* ***value*** в режимі інтерфейсного настройки. Це значення може

перебувати в діапазоні між 1 і 200 000 000. Наприклад, ***spanning-tree cost 25*** в режимі налаштування ***інтерфейсу***. Щоб повернути вартість порту до значення за замовчуванням, треба ввести в тому ж режимі команду ***no spanning-tree cost.***

У прикладі на рисунку 5.19 вартість внутрішнього кореневого шляху від S2 до кореневого моста S1 по шляху 1 дорівнює 19 (на основі зазначеної IEEE вартості індивідуального порту), а вартість внутрішнього кореневого шляху для шляху 2 дорівнює 38. Оскільки загальна вартість шляху 1 до кореневого мосту нижче, саме цей шлях є кращим. Протокол STP блокує резервний шлях, щоб уникнути формування петлі.

Щоб перевірити порт і вартість внутрішнього кореневого шляху до кореневого мосту використовують команду *show spanning-tree*. Поле вартості (Cost) у верхній частині вихідних даних являє собою вартість внутрішнього кореневого шляху – загальну вартість шляху до кореневого мосту. Це значення змінюється в залежності від кількості портів комутатора, які необхідно пройти на шляху до кореневого мосту. У вихідних даних все інтерфейси також визначені зі значенням вартості окремого порту 19.

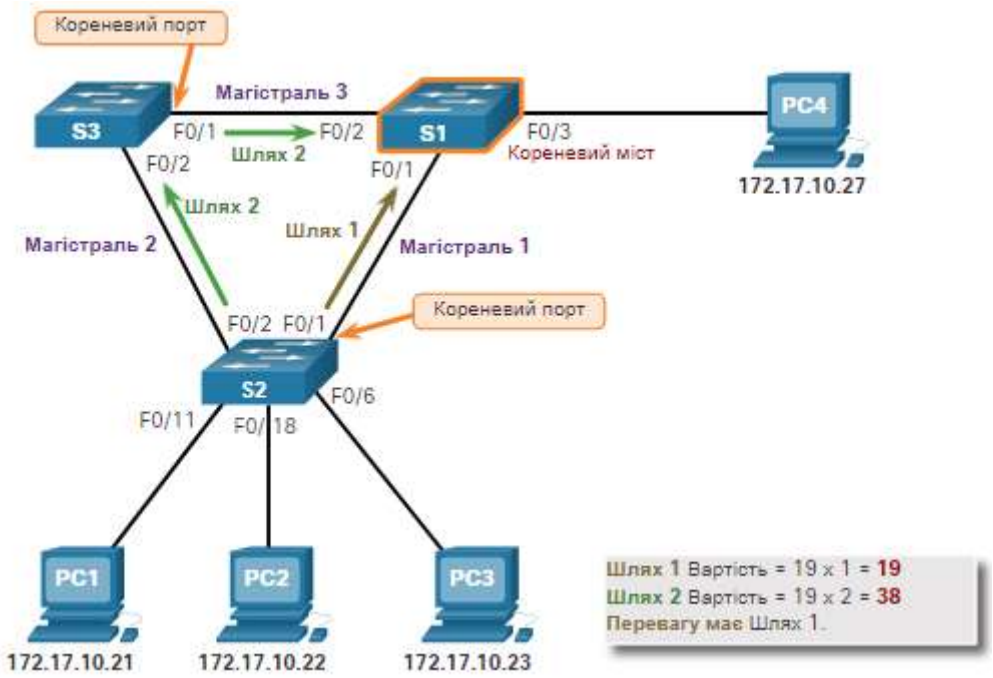


Рисунок 5.19 – Визначення вартості шляхів

На кореневому мосту не буде ніяких кореневих портів – всі порти на кореневому мосту будуть призначеними. Для комутатора, який не є кореневим мостом топології мережі, буде визначено лише один кореневий порт (рисунок 5.20).

Якщо два зустрічних порти визначені як призначені, то одних з них (з більшим BID) стає альтернативним портом, тобто блокується. Крім того враховується значення вартості шляху до кореневого мосту з певного інтерфейсу, а також вартість самого інтерфейсу.

Альтернативний порт не відправляє і не приймає трафік на цьому сегменті. Він працює як частина STP для запобігання утворенню петель.

В процесі роботи протоколу STP топологія мережі може змінюватися, це впливає на вартість шляхів та інші показники протоколу. Після змін параметрів для визначення нового кореневого моста всі наступні кадри BPDU, що відправляються з відповідного комутатора, містять новий кореневий ідентифікатор і нову вартість кореневого шляху. Таким чином, всі інші суміжні комутатори можуть постійно бачити найнижче значення ідентифікатора кореневого моста. У міру проходження кадрів BPDU між іншими суміжними комутаторами вартість шляху постійно оновлюється, щоб вказати загальну вартість шляху до кореневого мосту. Всі комутатори в протоколі spanning tree використовують свій шлях для визначення оптимального шляху до кореневого мосту.

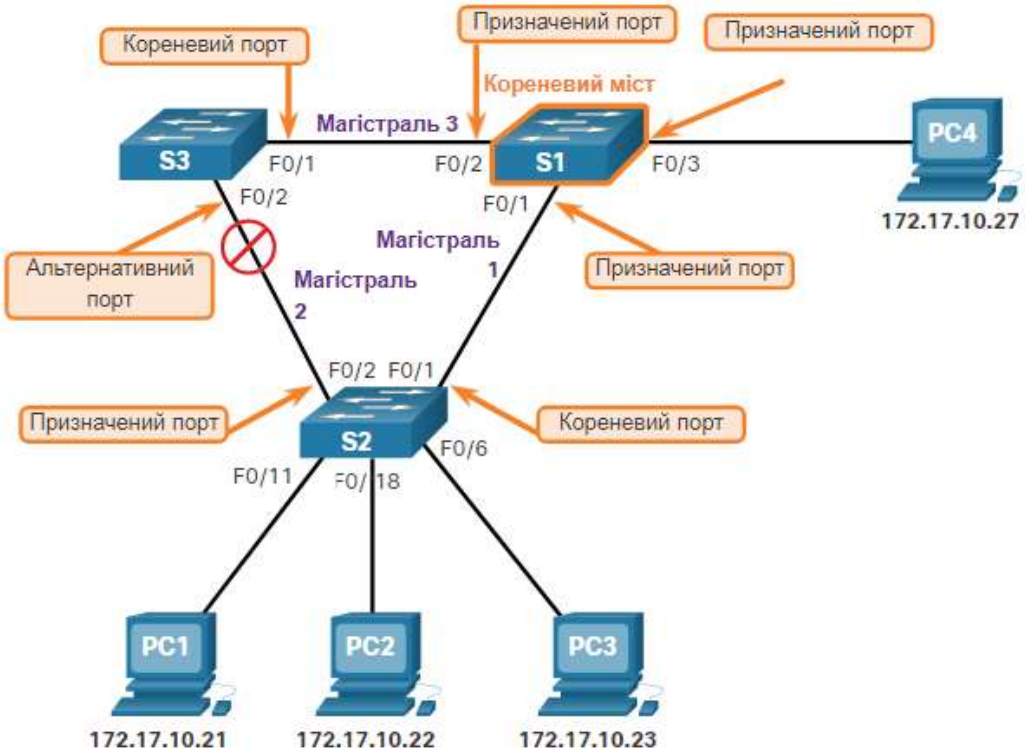


Рисунок 5.20 – Розподіл функцій портів

5.2.3. Сучасні версії протоколу STP, їхні особливості

З моменту створення вихідного стандарту IEEE 802.1D було розроблено кілька різновидів протоколів STP.

До різновидів протоколів STP відносяться наступні:

– STP. Це початкова версія IEEE 802.1D (802.1D-1998 і більш рання), яка запобігає формуванню петель в топології мережі з резервними каналами. Загальний протокол spanning-tree (CST): передбачає використання тільки одного примірника протоколу spanning-tree для всієї мережі з мостовим з’єднанням незалежно від кількості мереж VLAN.

– Швидкий протокол STP (RSTP) або IEEE 802.1w: доопрацьований протокол STP, який забезпечує більш швидке сходження, ніж протокол STP. 802.1D-2004: оновлена версія стандарту STP, в яку входить IEEE 802.1w.

– PVST+ є вдосконаленим протоколом компанії Cisco, в якому для кожного окремого VLAN використовується окремий екземпляр RSTP. Розглянутий варіант протоколу spanning-tree підтримує PortFast, UplinkFast, BackboneFast, BPDU guard, BPDU filter, root guard і loop guard.

– Rapid PVST+ – вдосконалений корпорацією Cisco протокол RSTP, який використовує PVST +. Rapid PVST + надає окремий екземпляр 802.1w для кожної мережі VLAN. Кожен окремий екземпляр підтримує функції PortFast, BPDU guard, BPDU filter, root guard і loop guard.

– Протокол множинного єднального дерева (Multiple Spanning Tree Protocol, MSTP) – це стандарт IEEE, натхненний ранньою фірмовою версією протоколу, Multiple Instance STP (MISTP), розробленого Cisco. MSTP поєднує декілька VLAN у одному екземплярі єднального дерева.

– Множинне єднальне дерево (Multiple Spanning Tree, MST) — це реалізація MSTP компанії Cisco, яка надає до 16 екземплярів RSTP і поєднує декілька VLAN з однаковою фізичною і логічною топологією у спільному екземплярі RSTP. Кожен екземпляр підтримує PortFast, захист BPDU, фільтр BPDU, захист кореня і захист від петель.

Мережному фахівцю, який відповідає за адміністрування комутаторів, треба прийняти рішення щодо того, який тип протоколу STP необхідно реалізувати. Деякі характеристики версій протоколу STP наведені в таблиці 5.3.

Таблиця 5.3 – Характеристики версій протоколу STP

Протокол	**Стандарт**	**Потрібні ресурси**	**Конвергенція**	**Розрахунок дерева**
STP	802.1D	Низкі	Повільна	Одне
PVST+	Cisco	Високі	Повільна	На VLAN
RSTP	802.1w	Середні	Висока	На VLAN
Rapid PVST+	Cisco	Дуже високі	Висока	На VLAN
MSTP	802.1s, Cisco	Середні	Висока	На екземпляр (декілька VLAN)

5.2.4. Налаштування протоколу STP

За замовченням протокол STP на комутаторах Cisco включений і має параметри, наведені в таблиці 5.4.

Таблиця 5.4 – Параметри протоколу STP за замовченням

Функція	**Налаштування**
Стан	Включений для VLAN 1
Версія	PVST+
Пріоритет комутатора	32768
Пріоритет дерева (на інтерфейсі)	128
Вартість інтерфейсів	1 Гбіт/с – 4; 100 мбіт/с – 19; 10 мбіт/с – 100
Пріоритет VLAN	128
Вартість портів VLAN	1 Гбіт/с – 4; 100 мбіт/с – 19; 10 мбіт/с – 100
Таймери	Привітання – 2 с; Час затримки – 15 с Час старіння – 20 с; Лічильник утримання – 6 BPDU

Якщо адміністратор планує налаштувати окремий комутатор в якості кореневого моста, значення пріоритету моста за замовченням необхідно скоригувати таким чином, щоб воно було нижче значень пріоритету моста для всіх інших комутаторів в мережі. Існує два різних методи налаштування значення пріоритету моста для комутаторів Cisco.

Метод 1

Для забезпечення отримання комутатором найменшого значення пріоритету моста застосовують команду ***spanning-tree vlan*** *vlan-id* ***root primary*** в режимі глобальної настройки. Пріоритет комутатора налаштовується за використанням попередньо певного значення 24576 або найбільшого значення, кратного 4096, яке менше найнижчого значення пріоритету моста, виявленого в мережі.

Якщо потрібний альтернативний кореневої міст, застосовують команду ***spanning-tree vlan*** *vlan-id* ***root secondary*** режиму глобальної настройки. Ця команда задає для комутатора попередньо певне значення пріоритету 28672. Таким чином, альтернативний комутатор стає кореневим мостом в разі відмови основного кореневого моста. При цьому мається на увазі, що для інших комутаторів в мережі визначено значення пріоритету за умовчанням 32768.

На рисунку 5.21 комутатор S1 призначений в якості основного кореневого моста за допомогою команди spanning-tree vlan 1 root primary, а комутатор S2 в якості допоміжного кореневого моста за допомогою команди spanning-tree vlan 1 root secondary.

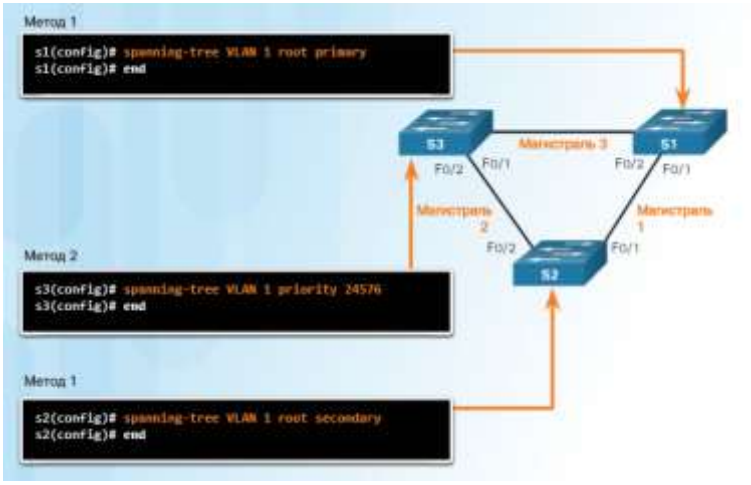


Рисунок 5.21 – Призначення кореневих функцій в мережі

Метод 2

Інший спосіб настройки значення пріоритету моста – використовувати команду режиму глобальної настройки ***spanning-tree vlan*** *vlan-id* ***priority*** *value*. Ця команда забезпечує більш ретельний контроль значення пріоритету моста. Значення пріоритету налаштовується за кроком в 4096 в діапазоні від 0 до 61440.

У цьому прикладі (рисунок 5.21) комутатору S3 присвоєно значення пріоритету моста 24576 за допомогою команди spanning-tree vlan 1 priority 24576.

Щоб перевірити пріоритет моста для комутатора, застосовують команду ***show spanning-tree***. На рисунку 5.22 для комутатора заданий пріоритет 24576 і він призначений в якості кореневого моста для примірника протоколу spanning-tree.

```
S3# show spanning-tree
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID     Priority    24577
              Address     000A.0033.3333
              This bridge is the root
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
  Bridge ID   Priority    24577  (priority  24576  sys-id-ext  1)
              Address     000A.0033.3333
              Hello Time  2 sec Max Age 20 sec Forward Delay 15 sec
              Aging Time  300

Interface     Role    Sts    Cost     Prio.Nbr   Type
------------  -----   ----   -----    ---------- ------
Fa0/1         Desg    FWD    4        128.1      p2p
Fa0/2         Desg    FWD    4        128.2      p2p
```

Рисунок 5.22 – Перегляд налаштувань STP

PortFast і BPDU Guard

PortFast є функцією Cisco для середовищ PVST+. Якщо порт комутатора налаштований за допомогою функції PortFast, то такий порт відразу переходить зі стану блокування в стан пересилання, минаючи стандартні стану переходу STP 802.1D (стану прослуховування та завантаження даних). Замість того, щоб очікувати сходження протоколу STP

IEEE 802.1D в кожній мережі VLAN, PortFast можна використовувати на портах доступу для забезпечення негайного підключення цих пристроїв до мережі. Портами доступу є порти, підключені до однієї робочої станції або сервера.

Оскільки PortFast призначений для мінімізації часу очікування портами доступу сходження протоколу spanning-tree, цю функцію рекомендується використовувати тільки на портах доступу. Якщо функція PortFast включена на порту, підключеному до іншого комутатора, виникне ризик виникнення петлі протоколу spanning-tree.

У допустимої конфігурації PortFast прийом кадрів BPDU ніколи не допускається, оскільки це вказувало б на те, що до порту підключений інший міст або комутатор, а це може привести до виникнення петлі протоколу spanning-tree. Комутатори Cisco підтримують функцію BPDU guard. Коли функція BPDU guard включена, при отриманні блоку BPDU вона переводить порт в стан errdisabled (error-disabled – відключення через помилку). Це дозволяє виключити порт. Функція BPDU guard забезпечує безпечний відгук на неприпустимі конфігурації.

Технологію Cisco PortFast рекомендується використовувати для DHCP. Без PortFast комп'ютер може відправити запит DHCP до переходу порту в стан пересилання, забороняючи вузлу отримувати придатний для використання IP-адресу та інші дані. Оскільки PortFast відразу ж змінює стан на стан пересилання, комп'ютер завжди отримує придатний для використання IP-адреса (Якщо DHCP-сервер налаштований правильно і відбувся обмін даними з DHCP-сервером).

Щоб налаштувати на порту комутатора PortFast, виконують команду режиму конфігурації інтерфейсу ***spanning-tree portfast*** на кожному інтерфейсі, для якого потрібно включити PortFast, як показано на рис 2. Команда глобального режиму конфігурації ***spanning-tree portfast default*** використовується для включення PortFast на всіх нетранкових інтерфейсах.

Щоб налаштувати BPDU guard на порту доступу 2-го рівня, використовують команду режиму конфігурації інтерфейсу ***spanning-tree bpduguard enable***. Команда глобального режиму конфігурації ***spanning-tree portfast bpduguard default*** включає BPDU guard на всіх портах з підтримкою PortFast.

Щоб перевірити, чи включений PortFast і BPDU для порту комутатора, використовують команду **show running-config**.

Контрольні питання до розділу 5

1. Охарактеризуйте протокол CDP (завдання, порядок роботи, особливості застосування).
2. Охарактеризуйте протокол ICMP (завдання, порядок роботи, особливості застосування).
3. Перерахуйте та поясніть варіанти ролей портів в протоколі STP.
4. Поясніть порядок вибору кореневого мосту та кореневих портів.
5. Поясніть порядок вибору альтернативних портів.

РОЗДІЛ 6
РЕАЛІЗАЦІЯ ТА ЗАСТОСУВАННЯ СПИСКІВ КОНТРОЛЮ ДОСТУПУ ACL

6.1. Реалізація контролю доступу з використанням ACL

6.1.1. Завдання та види ACL

Список контролю доступу (ACL) – це послідовний список правил дозволу або заборони, застосованих до інформаційних пакетів, відповідно до зазначених в них IP-адрес або ознак протоколів більш високого рівня. ACL-списки дозволяють ефективно контролювати трафік мережі на вході або виході маршрутизаторів. ACL-списки можна настроювати для усіх протоколів мережі, що маршрутизуються.

ACL-список реалізують послідовністю команд IOS, які визначають виходячи з інформації в заголовку пакету, чи пересилає маршрутизатор пакети чи скидає їх. ACL-списки є однією з найбільш використовуваних функцій операційної системи Cisco IOS.

На рисунку 6.1 наводиться приклад топології з використанням ACL-списків.

Залежно від конфігурації ACL-списки виконують наступні завдання:

– *Обмеження мережного трафіку* для підвищення продуктивності мережі. Наприклад, якщо корпоративна політика забороняє відеотрафік в мережі, необхідно настроїти і застосувати ACL-списки, блокуючі цей тип трафіку. Подібні заходи значно знижують навантаження на мережу і підвищують її продуктивність.

– *Управління потоком трафіку.* ACL-списки можуть обмежувати доставку оновлень маршрутизації. Такі налаштування мережі, дозволяють уникнути зайвого використання смуги пропускання.

– *Забезпечення базового рівня безпеки* відносно доступу до мережі. ACL-списки можуть відкрити доступ до частини мережі одному вузлу і закрити його для інших вузлів. Наприклад, доступ до мережі відділу кадрів може бути обмежений і дозволений тільки авторизованим користувачам.

– *Фільтрування трафіку на основі його типу*. Наприклад, ACL-список може дозволяти трафік електронної пошти, але при цьому блокувати увесь трафік протоколу Telnet.

– Списки контролю доступу здійснюють сортування вузлів в цілях *дозволу або заборони доступу до мережних служб*. За допомогою ACL-списків можна дозволяти або забороняти доступ до певних типів файлів, наприклад FTP або HTTP.

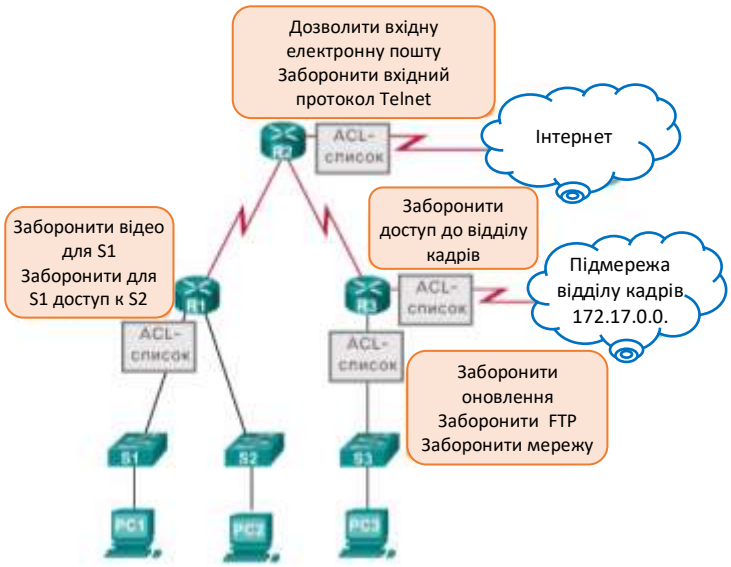


Рисунок 6.1 – Топології з використанням ACL-списків

За замовчанням ACL-списки не конфігуровані на маршрутизаторі, тому маршрутизатор не фільтрує трафік. Трафік, що поступає на маршрутизатор, маршрутизується виключно на основі інформації таблиці маршрутизації. *Проте якщо ACL-список використовується на інтерфейсі, маршрутизатор виконує додаткове завдання, оцінюючи усі мережні пакети, що проходять через інтерфейс, з метою визначення дозволу пересилки пакету.*

Типи ACL-списків Cisco для IPv4

Існує два типи ACL-списків Cisco для IPv4: ***стандартні і розширені*** ACL-списки.

Стандартні ACL-списки можна використати для дозволу або відхилення проходження трафіку тільки на основі IPv4-адрес джерела. *Адреса призначення пакету і порти, що беруть участь в передачі даних,* ***не оцінюються.*** У прикладі на рисунку 6.2 команда створення списку, що дозволяє увесь трафік від мережі 192.168.30.0/24. Стандартні ACL-списки створюються в режимі глобальної конфігурації.

```
access-list 10 permit 192.168.30.0 0.0.0.255
```

Рисунок 6.2 – Приклад стандартного ACL-списку

Розширені ACL-списки фільтрують IPv4-пакети, виходячи з декількох ознак:

- тип протоколу;
- IPv4-адреси джерела;
- IPv4-адреси призначення;
- TCP або UDP порти джерела;
- TCP або UDP порти призначення;
- додаткова інформація про тип протоколу.

На рисунку 6.3 розширений ACL-список 103 дозволяє трафіку з будь-якої адреси мережі 192.168.30.0/24 йти у будь-яку IPv4-мережу, якщо порт призначення – 80 (HTTP). Розширені ACL-списки створюються в режимі глобальної конфігурації.

```
access-list 103 permit tcp 192.168.30.0 0.0.0.255 any eq 80
```

Рисунок 6.3 – Приклад розширеного ACL-списку

Стандартні і розширені списки контролю доступу можна ***створювати з номером або іменем*** для ідентифікації ACL-списку і списку його правил.

Використання нумерованих ACL-списків – ефективний спосіб визначення типу ACL-списку в невеликих мережах, де в основному використовується трафік одного типу. Проте номер не містить інформації про призначення ACL-списку. З цієї причини, для визначення списків контролю доступу Cisco використовується присвоєне ім’я списку. Іменовані списки створюються у режимі часткового конфігурування.

Існують такі правила привласнення імен і номерів ACL-списків:

a. нумерований список:

- номери від 1 до 99 та від 1300 до 1999 – стандартний ACL-список;
- номери від 100 до 199 та від 2000 до 2699 – розширений ACL-список;

b. іменований список:

- імена можуть містити літерно-цифрові символи;
- рекомендовано використовувати ВЕЛИКИ ЛІТЕРИ;
- в іменах заборонені пробіли та знаки пунктуації;
- записи ACL-списку можна додавати і видаляти.

6.1.2. Принцип роботи та правила застосування ACL

Маршрутизатор працює як фільтр пакетів, коли перенаправляє або відкидає пакети на основі правил фільтрації. Фільтрація пакетів може здійснюватися на різних рівнях (3 та 4 – мережному та транспортному рівнях) моделі взаємодії відкритих систем (OSI) або на рівні міжмережного протоколу TCP/IP.

Для оцінки мережного трафіку, ACL-список перевіряє наступну інформацію із заголовка пакету рівня 3:

– IP-адреса джерела;
– IP-адреса призначення;
– тип повідомлення.

ACL-список також може перевіряти інформацію більш високого рівня із заголовка рівня 4, включаючи:

– порт джерела TCP/UDP;
– порт призначення TCP/UDP.

Списки контролю доступу забезпечують додатковий контроль над пакетами, які приймаються інтерфейсами, транзитними пакетами, які передаються через маршрутизатор, а також пакетами, які вирушають з інтерфейсів маршрутизатора. Списки контролю доступу не застосовуються до пакетів, створених маршрутизатором.

ACL-списки застосовують до трафіку, що входить або виходить:

– **ACL-списки по входу** – пакети, що входять, обробляються перед відправкою на вихідний інтерфейс. ACL-список по входу ефективний, оскільки він зберігає ресурси на пошук маршруту, якщо пакет скидається. Якщо пакет успішно проходить перевірку, він передається на обробку для подальшої маршрутизації. Вхідні ACL-списки є оптимальним рішенням для фільтрації пакетів, коли мережа, яка підключена до вхідного інтерфейсу, є єдиним джерелом пакетів, що вимагають аналізу.

– **ACL-списки по виходу** – пакети, що виходять, маршрутизуються на вихідний інтерфейс, а потім обробляються вихідним списком контролю доступу. ACL-списки по Вихідні краще всього використовувати, коли однакові фільтри застосовуються до пакетів, що поступають з безлічі інтерфейсів, що входять, перед виходом на один вихідний інтерфейс.

Останній запис будь-якого ACL-списку – це завжди "неявна відмова" (цей рядок напряму не вказують). Це правило автоматично вставляється в кінець кожного ACL-списку, хоча і не є присутнім в ньому фізично. Непряма відмова блокує увесь трафік. Унаслідок цієї неявної заборони ACL-список, що не містить хоч би одного дозволяючого правила, блокує увесь трафік.

Логіка стандартного ACL-списку

На рисунку 6.4 наведений алгоритм обробки пакетів, що поступають на маршрутизатор через інтерфейс G0/0. Перевірки адрес їх джерела здійснюються на основі наступних записів у списку:

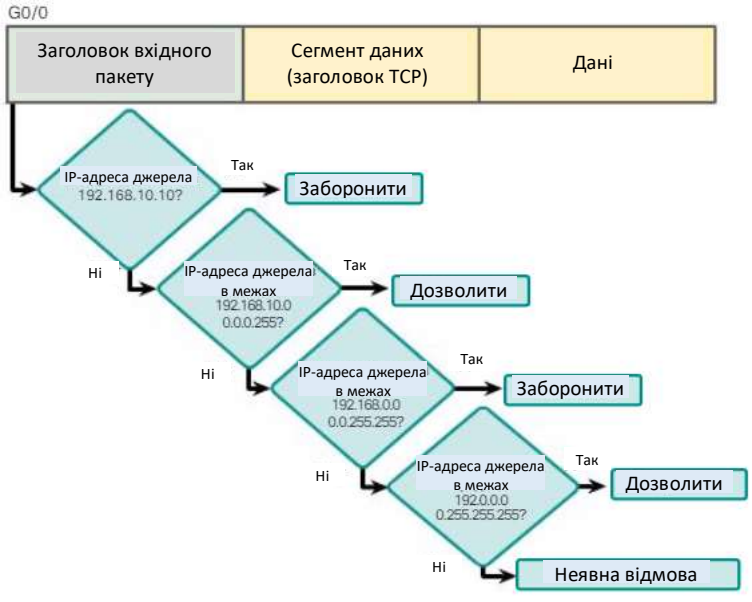


Рисунок 6.4 – Алгоритм обробки пакетів стандартним ACL-списком

access-list 2 deny 192.168.10.10
access-list 2 permit 192.168.10.0 0.0.0.255
access-list 2 deny 192.168.0.0 0.0.255.255
access-list 2 permit 192.0.0.0 0.255.255.255

Якщо пакети дозволені, вони прямують через маршрутизатор до вихідного інтерфейсу. Якщо пакети блокуються, вони відкидаються на вхідному інтерфейсі.

Основні правила застосування ACL-списків на маршрутизаторі:

Для кожного інтерфейсу може існувати декілька правил, необхідних для управління типами трафіку, яким дозволено входити або виходити через певний інтерфейс. Якщо маршрутизатор має два інтерфейси, зконфігурованих і для IPv4 і для IPv6. Якщо для обох протоколів потрібні ACL-списки на обох інтерфейсах і в обох напрямах, то потрібно буде створити 8 окремих ACL-списків. Кожен інтерфейс матиме чотири ACL-списки: два списки для протоколу IPv4 і два – для протоколу IPv6. Для кожного протоколу потрібний один ACL-список для трафіку, що входить, і один – для вихідного трафіку.

Рекомендації по використанню ACL-списків:

– Доцільно використовувати ACL-списки в міжмережних екранах маршрутизаторів, розміщених між внутрішньою мережею і зовнішньою мережею, наприклад Інтернетом.

– Для управління трафіком, що входить або виходить, в певній частині внутрішньої мережі треба використовувати ACL-списки на маршрутизаторі, розташованому між двома частинами мережі.

– ACL-списки доцільні на пограничних маршрутизаторах, тобто маршрутизаторах, розташованих на межах мереж.

– ACL-списки потрібні для кожного протоколу мережі, налагодженого на інтерфейсі пограничного маршрутизатора.

Правильне розміщення ACL-списку може підвищити ефективність мережі. ACL-список можна розмістити для мінімізації надмірного трафіку (рисунок 6.5):

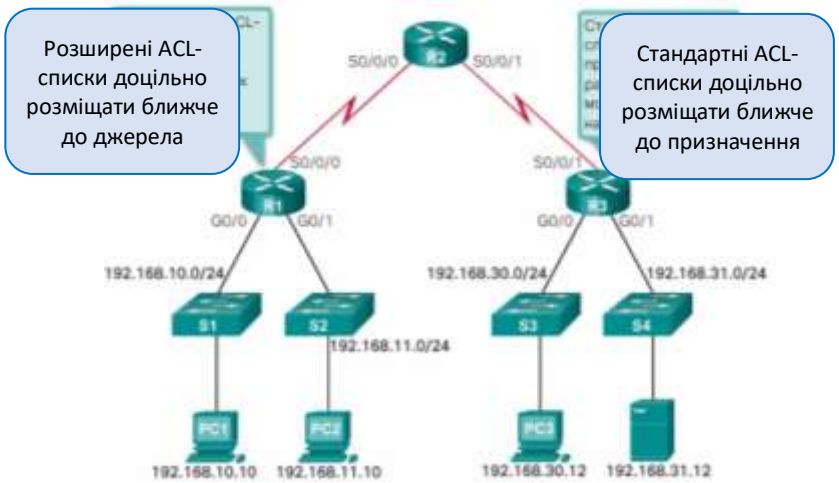


Рисунок 6.5 – Розміщення ACL-списку для мінімізації надмірного трафіку

– **Розширені ACL-списки** слід розміщувати максимально близько до джерела фільтрованого трафіку. Таким чином, небажаний трафік відхиляється близько до мережі-джерела, не перетинаючи інфраструктуру мережі.

– **Стандартні ACL-списки** – розміщують максимально близько до місця призначення. Розміщення стандартного ACL-списку у джерела трафіку дозволяє запобігти досягненню цим трафіком інших мереж через інтерфейс, на якому застосований ACL-список.

Коли трафік поступає на маршрутизатор, він порівнюється із записами в порядку, заданому в ACL-списку. Маршрутизатор продовжує обробку списку, поки не виявить збіг. Маршрутизатор обробляє пакет на основі першого знайденого збігу, інші записи маршрутизатором не враховуються.

Якщо до кінця списку збігу не знайдені, маршрутизатор відхиляє трафік.

6.1.3. Формат команд для реалізації та редагування ACL

Налаштування стандартних ACL-списків

Для використання стандартних нумерованих ACL-списків на маршрутизаторі Cisco необхідно спочатку створити стандартний ACL-список і потім активувати його на інтерфейсі.

Команда глобальної конфігурації **access-list** визначає стандартний ACL-список з номером в діапазоні від 1 до 99. У ОС Cisco IOS версії 12.0.1 цей діапазон розширений; для стандартних ACL-списків можуть використовуватися номери від 1300 до 1999. Це дозволяє створити до 798 можливих стандартних ACL-списків. Додаткові номери посилаються на розширений ACL-список по протоколу IP.

Нижче наводиться повний синтаксис команди стандартного ACL-списку:

Router(config)# **access-list** *access-list-number* {**deny** | **permit** | **remark**}*source* [*source-wildcard*][**log**]

Записи можуть дозволити (**permit**) або заборонити (**deny**) окремий вузол або діапазон адрес вузлів. Для створення в нумерованому ACL-списку 10 запису, що дозволяє певний вузол з IP-адресом 192.168.10.0, необхідно ввести наступну команду:

R1(config)#**access-list 10 permit host 192.168.10.10**

Для створення запису, який дозволить діапазон IPv4-адресів в нумерованому ACL-списку 10, що дозволяє усі IPv4-адреси в мережі 192.168.10.0/24, необхідно ввести наступну команду:

R1(config)# **access-list 10 permit 192.168.10.0 0.0.0.255**

Для видалення ACL-списку використовується команда глобальної конфігурації **no access-list**. Введення команди **show access-list** показує всі наявні ACL-списки.

Для документування і спрощення прочитання ACL-списків використовується ключове слово **remark**. Довжина коментаря обмежена 100 символами.

Ключові слова **host** й **any** в командах створення списків спрощують завдання, допомагаючи визначити найчастіше використовувану шаблонну маску. Ці ключові слова виключають необхідність введення шаблонних масок при визначенні конкретного вузла або цілої мережі. Ці ключові слова полегшують читання ACL-списку, надаючи візуальні підказки відносно критеріїв джерела або призначення.

Ключове слово **host** застосовується для маски 0.0.0.0. Ця маска вказує, що повинні співпадати усі біти IPv4-адреси, або співпадає тільки один вузол.

Ключове слово **any** застосовується для IP-адреси і маски 255.255.255.255. Ця маска вказує ігнорувати увесь IPv4-адрес або прийняти будь-яку адресу.

Наприклад, замість введення **192.168.10.10 0.0.0.0** можна ввести рядок **host 192.168.10.10**. Або замість інструкції **0.0.0.0 255.255.255.255** можна ввести окремо ключове слово **any.**

Із-за неявного правила **«deny any»** у кінці списку цей ACL-список блокує увесь інший трафік.

Створення стандартних іменованих ACL-списків

Привласнення імен ACL-спискам спрощує розуміння їх функцій. Наприклад, ACL-списку, налагодженому для заборони FTP, можна присвоїти ім’я «NO_FTP». При привласненні ACL-списку імені замість номера, режим конфігурації і синтаксис команд трохи міняються.

Крок 1. Для створенням іменованого ACL-списку потрібно виконати команду режиму глобальної конфігурації

Router(config)# **ip access-list** {**standard** | **extended**} *name*

Імена ACL-списків складаються з буквено-цифрових символів, вони чутливі до регістра і мають бути унікальними. Команда *ip access-list standard name* використовується для створення стандартного іменованого ACL-списку, тоді як команда *ip access-list extended name* застосовується для створення розширеного списку доступу. Після введення команди маршрутизатор входить в режим конфігурації іменованого ACL-списку.

Крок 2. У режимі конфігурації іменованих ACL-списків застосовуються команди *permit* або *deny*, щоб задати одне або більше за умови визначення відправки або відхилення пакету, у форматі наведеному нижче.

permit | deny *source* *source-wildcard*

Крок 3. ACL-список потрібно застосувати до інтерфейсу за допомогою команди **ip access-group** з визначенням, чи повинен ACL-список застосовуватися до пакетів, коли вони приходять на інтерфейс (*in*), або коли вони покидають його (*out*). Команда виконується в режимі часткового конфігурування відповідного інтерфейсу

ACL-статистика

Після застосування ACL-списку на інтерфейсі і завершення перевірки за допомогою команди **show access-lists** відображається статистика для кожного співпадаючого запису.

В процесі тестування ACL-списку, лічильники можна скинути, виконавши команду **clear access-list counters**. Цю команду можна застосовувати загалом або з вказівкою номера або імені конкретного ACL-списку.

Налаштування розширених ACL-списків

Послідовність кроків налаштування розширених ACL-списків така ж, як для стандартних ACL-списків. Спочатку розширений ACL-список настроюється, а потім активується на інтерфейсі. При цьому слід враховувати, що синтаксис команди і параметри складніші для забезпечення підтримки додаткових функцій, що надаються розширеними ACL-списками, а саме:

permit | deny *tcp* ***source*** *source-wildcard* [operator [port]] ***destination*** *destination-wildcard* [operator [port]] [established]

На рисунку 6.6 наведений приклад розширеного списку контролю доступу. В даному прикладі мережний адміністратор настроїв ACL-списки для обмеження мережного доступу будь-якої зовнішньої мережі, щоб дозволити перегляд веб-сайтів тільки з LAN, підключеної до G0/0. ACL 103 дозволяє трафік, який надходить від будь-якої адреси мережі 192.168.10.0, перейти до будь-якого місця призначення з урахуванням обмеження, що трафік використовує тільки порти 80 (HTTP) і 443 (HTTPS).

Характер протоколу HTTP вимагає, щоб трафік повертався назад в мережу від веб-сайтів, до яких зверталися внутрішні клієнти. Мережний адміністратор хоче обмежити трафік, що повертається, до HTTP-обмінів від запитаних веб-сайтів, забороняючи увесь інший трафік. Це завдання виконує ACL 104, блокуючи увесь трафік, що входить, за винятком трафіку від раніше встановлених підключень. Запис *permit* в ACL 104 дозволяє трафік, що входить, параметром *established*. Параметр established дозволяє повернення в мережу 192.168.10.0/24 тільки того трафіку, який запит на який спочатку виходив з цієї мережі. Пакет задовольняє умовам, якщо зворотний сегмент протоколу TCP має біти ACK і RST, які вказують, що пакет належить існуючому підключенню. Без параметра *established* запису ACL-

списку клієнт може послати трафік на веб-сервер, але не отримати зворотний трафік, що повертається від веб-сервера.

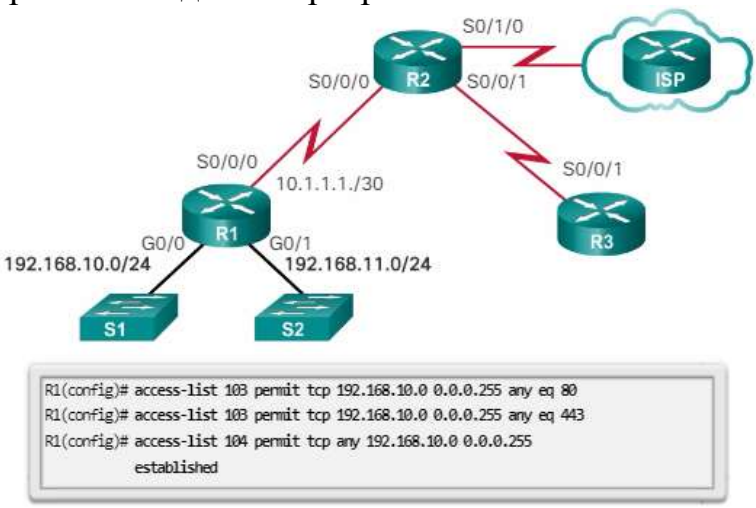


Рисунок 6.6 – Приклад розширеного списку контролю доступу

Застосування розширених ACL-списків на інтерфейсах

Навіть налагоджений ACL не фільтруватиме трафік до того, як буде застосований на інтерфейсі. Перед застосуванням ACL на інтерфейсі необхідно визначити, який вид трафіку фільтруватиметься: вхідний або вихідний. Коли користувач внутрішньої LAN дістає доступ до веб-сайту в Інтернеті, трафік йде в Інтернет. Коли внутрішній користувач отримує електронну пошту з Інтернету, трафік йде на локальний маршрутизатор. Проте у випадку із застосуванням списку контролю доступу на інтерфейсі, «in» і «out» набувають інших значень. З точки зору ACL-списку, «in» і «out» є посиланнями на інтерфейс маршрутизатора.

У топології, зображеної на рисунку 6.6, маршрутизатор R1 має три інтерфейси. Це послідовний інтерфейс S0/0/0 і два інтерфейси Gigabit Ethernet: G0/0 і G0/1. Враховуючи що розширений список контролю доступу зазвичай має бути застосований як можна ближче до джерела – у цій топології найближчий до джерела цільового трафіку інтерфейс G0/0.

Трафік веб-запитів від користувачів LAN 192.168.10.0/24 – трафік, що входить, на інтерфейс G0/0. Зворотний трафік від встановлених з’єднань до користувачів локальної мережі вважається вихідним з інтерфейсу G0/0. Приклад застосування ACL-списку на інтерфейсі G0/0 в обох напрямах зображений на рисунку 6.7. Вхідний ACL 103 перевіряє тип трафіку. Вихідний ACL 104 перевіряє трафік, що повертається від встановлених з’єднань. Це обмежує доступ в Інтернет для мережі 192.168.10.0, щоб дозволити тільки перегляд веб-сторінок.

Список доступу можна застосувати на інтерфейсі S0/0/0, але в цьому випадку при обробці списку контролю доступу маршрутизатор переглядатиме усі пакети, що приходять на нього, а не тільки трафік в мережу 192.168.11.0 і з неї. Це може стати причиною зайвого навантаження на маршрутизатор.

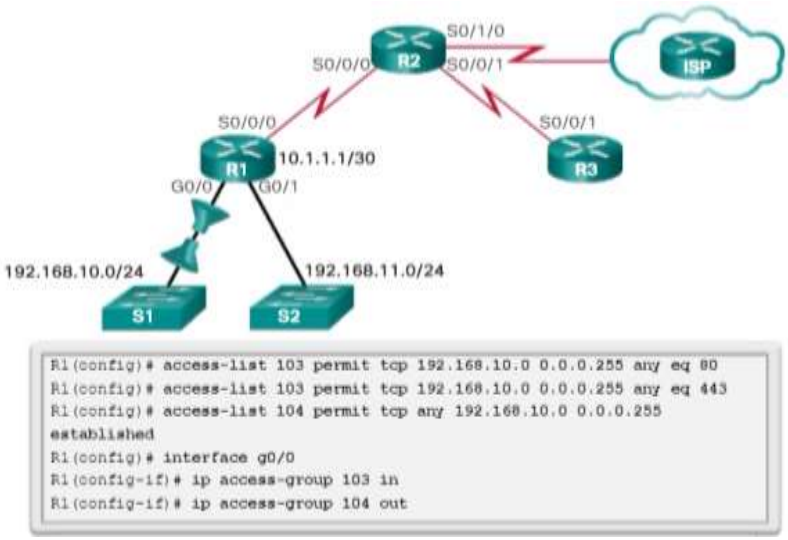


Рисунок 6.7 – Застосування ACL-списку на інтерфейсі

У прикладі на рисунку 6.8 заборонений трафік FTP з підмережі 192.168.11.0, який спрямовується в підмережу 192.168.10.0, але дозволений будь-який інший тип трафіку. При цьому використовується шаблонна маска і неявна команди відмови *deny any*. Протокол FTP використовує порти TCP 20 і 21; таким чином, для заборони доступу FTP ACL-списку потрібно обидва ключові слова імені порту: *ftp* і *ftp-data* або *eq 20* і *eq 21*.

Якщо використовується номер порту замість імені порту, команди матимуть наступний вигляд:

access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 20
access-list 114 permit tcp 192.168.20.0 0.0.0.255 any eq 21

Щоб виключити блокування усього трафіку командою *deny any*, представленою у вигляді непрямого запису у кінці кожного ACL-списку, необхідно додати команду **permit ip any any**. За відсутності, принаймні, однієї дозволяючої команди permit в ACL-списке увесь трафік на інтерфейсі, де застосований ACL, буде скинутий. Список контролю доступу повинен застосовуватися на інтерфейсі G0/1для того, щоб трафік, що входить з локальної мережі 192.168.11.0/24, фільтрувався при вході на інтерфейс маршрутизатора.

У прикладі на рисунку 6.9 заборонений трафік протоколу Telnet з будь-якого джерела в LAN 192.168.11.0/24, але дозволений увесь інший IP-трафік. Оскільки трафік, призначений для локальної мережі 192.168.11.0/24, є вихідним на інтерфейсі G0/1, ACL-список буде застосований на G0/1 з ключовим словом *out* і з використанням ключових слів *any* в командах дозволу. Запис, що містить дозвіл, додається, щоб уникнути непотрібного блокування трафіку.

У прикладах на рис. 6.8 і 6.9 у кінці ACL-списку наводиться команда permit ip any any. Для забезпечення більшої безпеки можна застосувати команду permit 192.168.11.0 0.0.0.255 any.

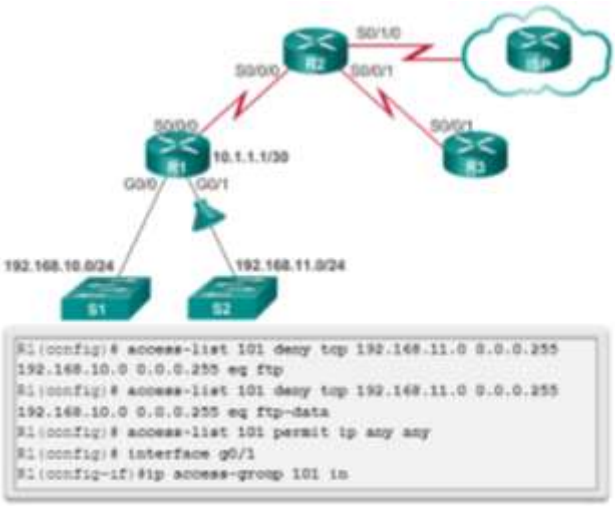


Рисунок 6.8 – ACL-список, заборони FTP

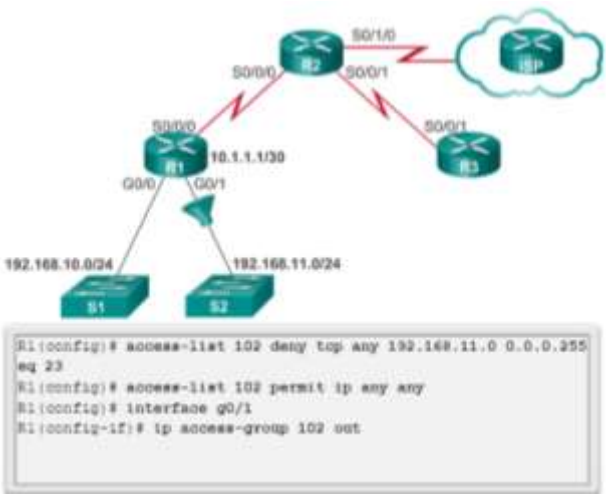


Рисунок 6.9 – ACL-список, заборони Telnet

Для редагування списку контролю доступу можна використовувати один з двох методів:

Метод 1. ***Текстовий редактор*** – при використанні цього методу ACL-список копіюється і вставляється в текстовий редактор, в якому виробляються зміни. Поточний список доступу видаляється командою **no access-list**. Відредагований ACL-список потім вставляється назад в конфігурацію.

Метод 2. ***Порядкові номери*** – порядкові номери використовуються для видалення або вставки записи списку контролю доступу. Команда **ip access-list** {**standard** | **extended**} *name (number)* використовується для переходу в режим настройки списку контролю доступу. Якщо списку контролю доступу присвоєно номер, а не ім’я, то цей номер потрібно вказати в параметрі. Записи можна вставити або видалити, використовуючи номери рядків. Для видалення використовують команду **no** *номер рядка*. Для додавання використовується стандартна команда для правила, але з необхідним номером на початку (рисунок 6.10).

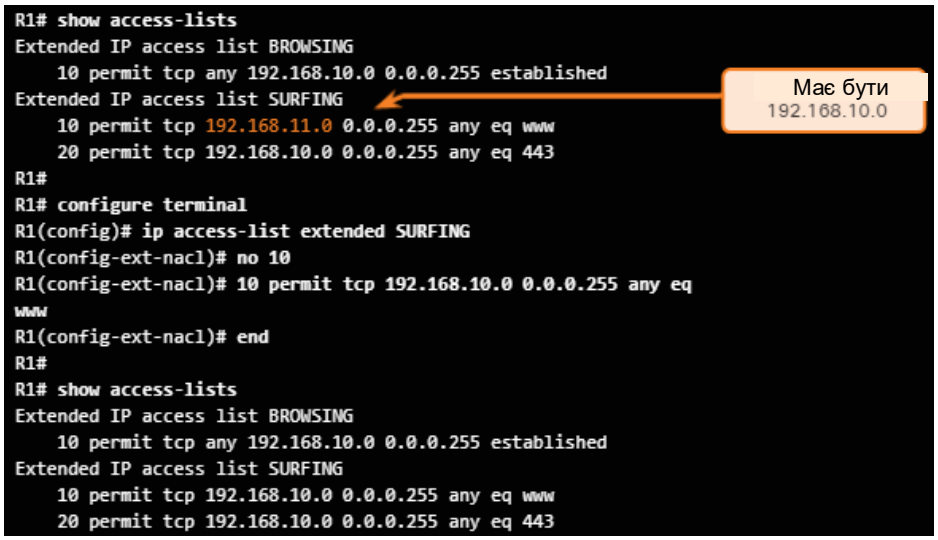


Рисунок 6.10 – Редагування ACL-списку

6.2. Протоколи перетворення адрес nat та pat

6.2.1. Призначення та види протоколів перетворення адрес

Кількості публічних IPv4-адресов недостатньо, щоб призначити унікальні адреси усім пристроям, підключеним до Інтернету. У більшості випадків локальні мережі реалізуються з використанням приватних IPv4-адресів відповідно до RFC 1918. Адресний простір часткових IPv4-адрес складається з 3 блоків:

- 10.0.0.0 … 10.255.255.255 (клас A);
- 172.16.0.0 … 172.31.255.255 (клас B);
- 192.168.0.0 … 192.168.255.255 (клас C).

Ці приватні адреси використовуються у рамках організації або об'єкту з метою забезпечення взаємодії пристроїв на локальному рівні. Але оскільки ці адреси не визначають конкретну компанію або організацію, приватні IPv4-адреса не можна використати для маршрутизації через Інтернет. Для того, щоб дозволити пристрою з приватною IPv4-адресою отримувати доступ до пристроїв і ресурсів поза локальною мережею, приватну адресу спочатку необхідно перетворити в публічну адресу.

NAT (Network Address Translation – «перетворення мережних адрес») забезпечує перетворення приватних адрес в публічні адреси. Це дозволяє пристрою з приватною IPv4-адресою діставати доступ до ресурсів поза своєю приватною мережею, включаючи ресурси в Інтернеті. У поєднанні з приватними IPv4-адресами NAT продемонстрував свою доцільність відносно економії публічних IPv4-адресов. Одна публічна IPv4-адреса може спільно використовуватися з сотнями, навіть тисячами пристроїв, для кожного з яких налагоджена унікальна приватна IPv4-адреса.

Термінологія NAT

У термінології NAT під "внутрішньою мережею" мається на увазі набір мереж, чиї адреси транслюватимуться. Термін "зовнішня мережа" відноситься до усіх інших мереж.

При використанні NAT IPv4-адреси представляють різні точки призначення залежно від того, де вони знаходяться: в приватній або в публічній мережі (Інтернет), а також від того, чи є трафік таким, що входить або вихідним.

У NAT передбачені 4 типи адрес:

- внутрішня локальна адреса;
- внутрішня глобальна адреса;
- зовнішня локальна адреса;
- зовнішня глобальна адреса.

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

– **Внутрішня (inside) адреса** – це адреса пристрою, яка перетворюється механізмом NAT.

– **Зовнішня (ouside) адреса** – це адреса обладнання призначення.

У рамках NAT по відношенню до адрес також використовується поняття локальності або глобальності:

– **Локальна адреса** – це будь-яка адреса, яка перебуває у внутрішній частині мережі.

– **Глобальна адреса** – це будь-яка адреса, яка перебуває в зовнішній частині мережі.

На рисунку 6.11 внутрішньою локальною адресою ПК 1 є 192.168.10.10. З точки зору ПК 1 веб-сервер використовує зовнішню адресу 209.165.201.1. Якщо пакети вирушають від ПК 1 на глобальну адресу веб-сервера, внутрішня локальна адреса ПК 1 перетворюється на 209.165.200.226 (внутрішня глобальна адреса). Адреса зовнішнього пристрою зазвичай не перетворюється, оскільки ця адреса зазвичай вже є публічною IPv4-адресою.

Отже, для ПК 1 використовуються різні локальна і глобальна адреси, а для веб-сервера в обох випадках використовується одна публічна IPv4-адреса. З точки зору веб-сервера трафік, вихідний від ПК 1, є таким, що надходить з адреси 209.165.200.226, внутрішньої глобальної адреси.

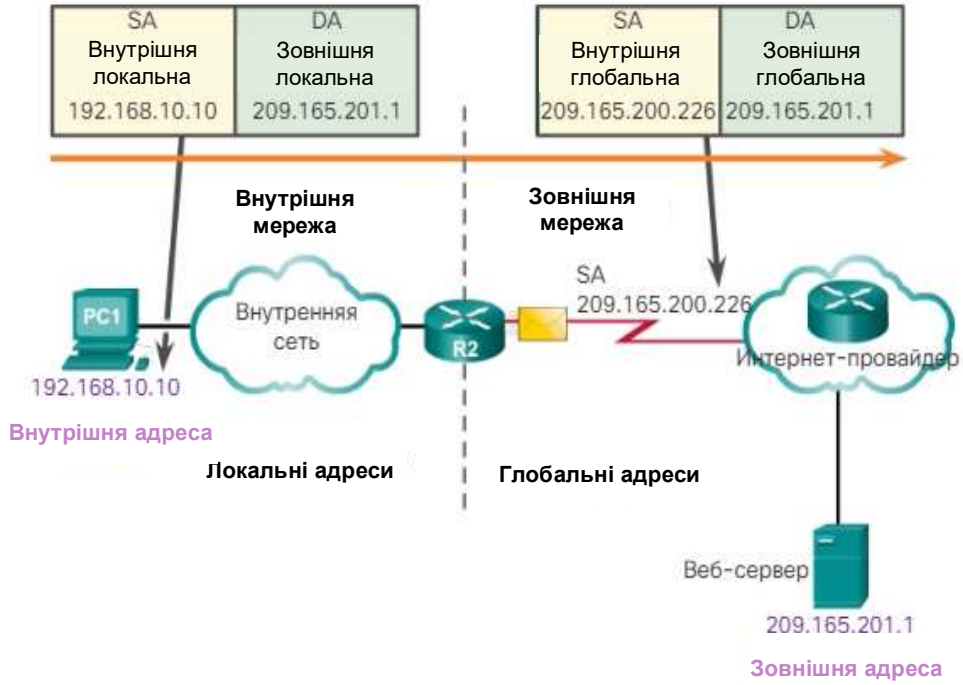


Рисунок 6.11 – Типи адрес NAT

Маршрутизатор NAT (R2 на рисунку 6.11) є точкою розмежування між внутрішньою і зовнішньою мережами, а також між локальними і глобальними адресами.

Існують три механізми перетворення:

– **Статичне перетворення (статичний NAT)** – це взаємно-однозначна відповідність між локальною і глобальною адресами.

– **Динамічне перетворення (динамічний NAT)** – це зіставлення адрес за схемою “багато до багатьох” між локальними і глобальними адресами.

– **Перетворення адреси і номера порту (PAT)** – це зіставлення адрес за схемою “багато до одного” між локальними і глобальною адресами. Цей метод також називається перевантаженням (NAT з перевантаженням).

Статичне перетворення NAT

Статичний NAT використовує зіставлення локальних і глобальних адрес за схемою «один в один». Ці відповідності задаються адміністратором мережі і залишаються незмінними.

На рисунку 6.12 у маршрутизаторі R2 налагоджені статичні відповідності для внутрішніх локальних адрес Svr1, ПК 2 і ПК 3. Коли ці пристрої відправляють трафік в Інтернет, їх внутрішні локальні адреси перетворюються в задані внутрішні глобальні адреси. Для зовнішніх мереж ці пристрої використовують публічні IPv4-адреса.

Метод статичного перетворення особливо корисний для веб-серверів або пристроїв, які повинні мати постійну адресу, доступну з Інтернету – наприклад, для веб-сервера компанії. Статичний NAT також підходить для пристроїв, які мають бути доступні авторизованому персоналу, працюючому поза офісом, але при цьому залишатися закритими для загального доступу через Інтернет. Наприклад, мережний адміністратор може з ПК 4 підключитися за допомогою SSH до внутрішньої глобальної адреси Svr1 (209.165.200.226). Маршрутизатор R2 перетворює цю внутрішню глобальну адресу у внутрішню локальну адресу і підключає сеанс адміністратора до Svr1.

Для статичного NAT потрібно достатню кількість публічних адрес, доступних для загальної кількості користувачів.

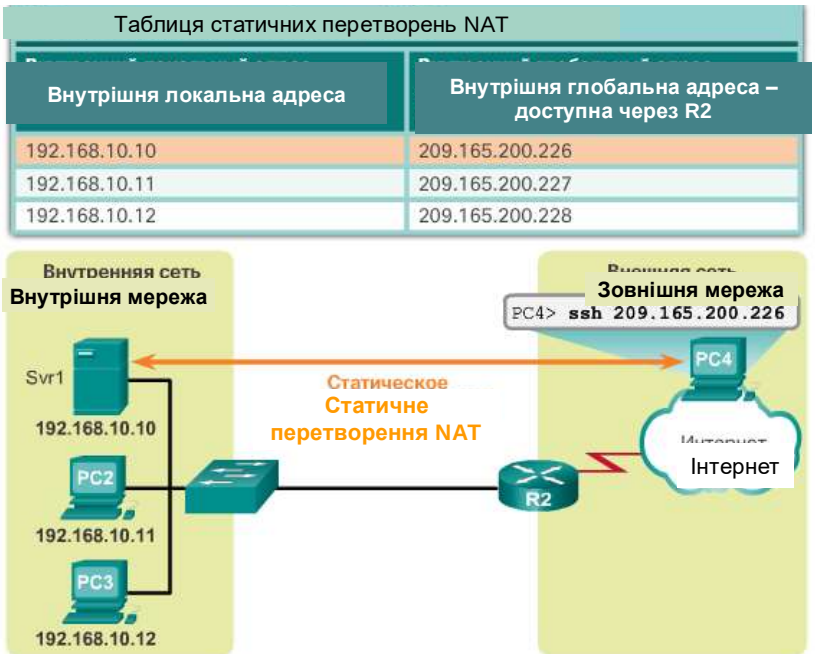


Рисунок 6.12 – Статичне перетворення NAT

Динамічне перетворення NAT

При динамічному перетворенні NAT використовується пул публічних адрес, які призначаються по черзі (“першим прийшов – першим обслужили”). Коли внутрішній пристрій просить доступ до зовнішньої мережі, динамічне перетворення NAT призначає доступний публічний IPv4-адрес з пулу.

На рисунку 6.13 PC3 дістає доступ до Інтернету, використовуючи першу доступну адресу в пулі динамічного NAT. Інші адреси як і раніше доступні для використання. Як і для статичного NAT, для динамічного NAT потрібно достатню кількість публічних адрес, здатну забезпечити загальну кількість одночасних сеансів користувачів.

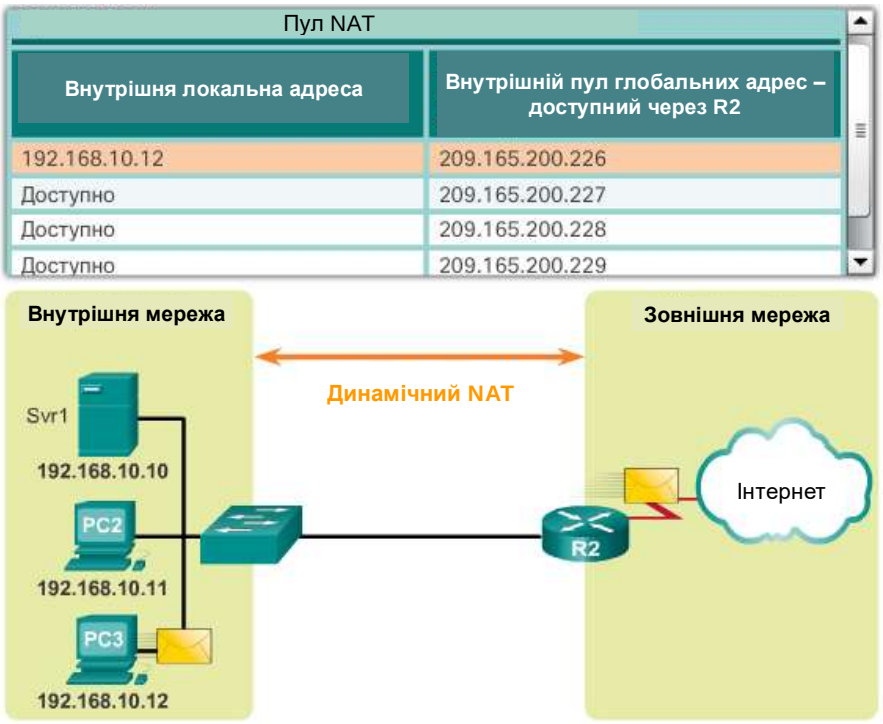


Рисунок 6.13 – Динамічне перетворення NAT

Перетворення адреси і номера порту (PAT)

Перетворення адреси і номера порту (PAT), також називають NAT з перевантаженням, зіставляє безліч приватних IPv4-адрес однієї або кільком публічним IPv4-адресам. Саме цей метод реалізується у більшості домашніх маршрутизаторів. Інтернет-провайдер призначає маршрутизатору одну адресу, але декілька членів сім’ї можуть одночасно одержувати доступ до Інтернету. NAT з перевантаженням – це найбільш поширений метод перетворення.

Якщо пристрій починає сеанс TCP/IP, PAT створює значення порту джерела TCP або UDP, щоб унікальним чином визначити сеанс. Якщо маршрутизатор NAT отримує пакет від клієнта, він використовує свій номер порту джерела, щоб унікальним чином визначити конкретне перетворення NAT.

PAT гарантує, що пристрої використовуватимуть різні номери портів TCP для кожного сеансу взаємодії з сервером в Інтернеті. При поверненні відповіді від сервера, номер порту джерела, який став номером порту призначення при зворотній передачі, визначає, якому пристрою маршрутизатор перешле відповідні пакети. Процес PAT також перевіряє, чи були замовлені пакети, які входять, таким чином підвищуючи безпеку сеансу.

Рисунок 6.14 ілюструє процес перетворення адрес портів (PAT). Щоб розрізняти перетворення, механізм PAT додає унікальні номери портів джерела до внутрішньої глобальної адреси.

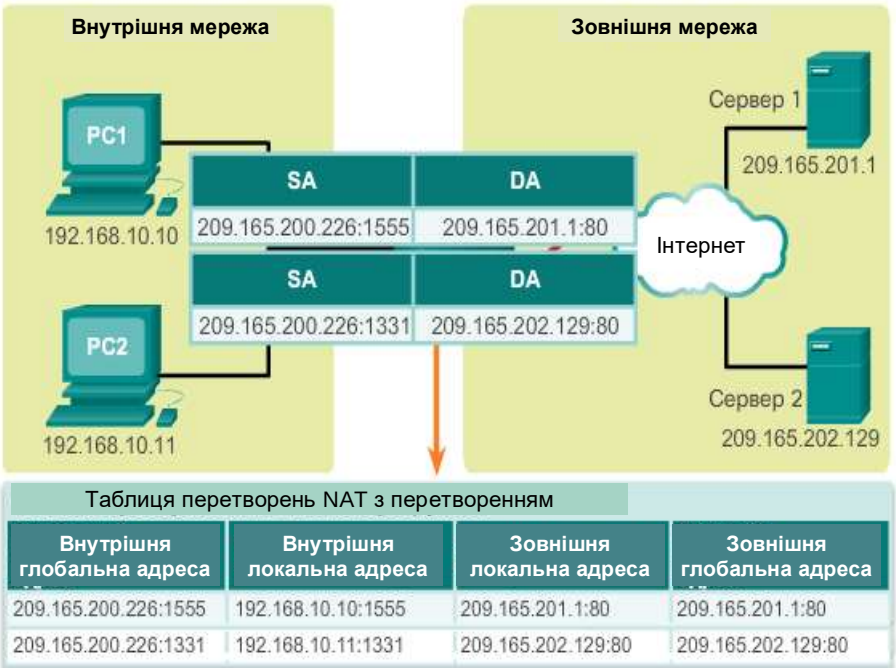


Рисунок 6.14 – Процес перетворення адрес портів (PAT)

Оскільки маршрутизатор R2 обробляє кожен пакет, він використовує номер порту (у даному прикладі 1331 і 1555) для ідентифікації пристрою, з якого поступив пакет. Адреса джерела (SA) – це внутрішня локальна адреса з доданим призначеним номером порту TCP/IP. Адреса призначення (DA) – це зовнішня локальна адреса з доданим номером порту необхідної служби. У цьому прикладі порт служби дорівнює 80, тобто порт для протоколу HTTP.

Маршрутизатор R2 перетворює внутрішню локальну адресу у внутрішню глобальну адресу з доданим номером порту. Адреса призначення не змінюється, але тепер вона вважається зовнішньою глобальною IP-адресою. Коли веб-сервер відповідає, шлях повторюється, тільки в зворотному порядку.

Перетворення PAT намагається зберегти первинний порт джерела. У тому випадку, якщо первинний порт джерела вже використовується, PAT призначає перший доступний номер порту, починаючи з найменшого у відповідній групі портів – 0…511, 512…1023 або 1024…65535. Якщо доступних портів більше немає, а в пулі адрес є декілька зовнішніх адрес,

PAT переходить до наступної адреси, намагаючись виділити первинний порт джерела. Цей процес триває до тих пір, поки не вичерпаються як доступні порти, так і зовнішні IP-адреси.

Примітка. Сумарна кількість внутрішніх адрес, які можуть бути перетворені в одну зовнішню адресу, теоретично може досягати 65536 на одну IP-адресу. Але на практиці кількість внутрішніх адрес, яким можна призначити одну IP-адресу, приблизно складає 4000.

6.2.2. Формат команд для реалізації та порядок застосування протоколів перетворення адрес

Налаштування статичного NAT

Налаштування статичного NAT зв'язане з двома основними завданнями.

Крок 1. Створення відповідності між внутрішньою локальною і внутрішньою глобальною адресами. Наприклад, на рисунку 6.12 в якості статичного перетворення NAT налагоджені внутрішня локальна адреса 192.168.10.10 і внутрішня глобальна адреса 209.165.200.226.

Крок 2. Після налаштування відповідності, інтерфейси, що беруть участь в перетворенні, настроюються як внутрішні або зовнішні відносно NAT. В даному прикладі це інтерфейси маршрутизатора R2: Ethernet – є внутрішнім, а Serial – зовнішнім інтерфейсом.

Пакети, що поступають на внутрішній інтерфейс маршрутизатора R2 від внутрішньої локальної IPv4-адреси (192.168.10.10), перетворюються, а потім передаються в зовнішню мережу. Пакети, що поступають на зовнішній інтерфейс маршрутизатора R2 (Serial) й адресовані до внутрішньої глобальної IPv4-адреси (209.165.200.226), перетворюються для передачі на внутрішню локальну адресу (192.168.10.10) і потім передаються у внутрішню мережу.

У таблиці 6.1 приведені команди, необхідні для налаштування статичного NAT.

Таблиця 6.1 – Послідовність команд для налаштування статичного NAT

Крок	Дія
1	Налаштування статичного перетворення між внутрішньою локальною адресою і внутрішньою глобальною адресою *Router(config)# **ip nat inside source static** local-ip global-ip*
2	Увійти в режим налаштування інтерфейсу, до якого підключена внутрішня мережа, та позначити його, як внутрішній *Router(config)# **interface** type number* *Router(config-if)# **ip nat inside***
	Увійти в режим налаштування інтерфейсу, до якого підключена зовнішня мережа, та позначити його, як зовнішній *Router(config)# **interface** type number* *Router(config-if)# **ip nat outside***

Для перевірки налаштування та роботи статичного перетворення NAT на маршрутизаторі використовують команду ***show ip nat translations***. Результат застосування такого перегляду наведений на рисунку 6.15.

```
R2# show ip nat translations
Pro Inside global  Inside local   Outside local  Outside global
--- 209.165.201.5  192.168.10.254  ---            ---
R2#
```

а.

```
R2# show ip nat translations
Pro Inside global Inside local   Outside local    Outside global
--- 209.165.201.5 192.168.10.254 209.165.200.254  209.165.200.254
R2#
```

б.

Рисунок 6.14 – Перевірка налаштування (а) та роботи (б) статичного перетворення NAT на маршрутизаторі

Налаштування динамічного NAT

Для налаштування динамічного NAT потрібно виконати такі дії:

Крок 1. За допомогою команди **ip nat pool** визначити пул адрес, які використовуватимуться для перетворення. Цей пул адрес зазвичай є групою публічних адрес. Ці адреси визначаються за допомогою вказівки початкової і кінцевої IP-адреси пулу. Ключове слово *netmask* або *prefix-length* вказує, які біти адреси відносяться до мережі, а які – до діапазону адрес вузлів.

Крок 2. Налаштувати стандартний ACL, щоб визначити (дозволити) тільки ті адреси, які мають бути перетворені.

Крок 3. Виконати прив’язку ACL до пулу. Команда **ip nat inside source list** *access-list-number* **pool** *pool name* використовується для прив’язки списку до пулу. Це налаштування використовується маршрутизатором, щоб визначити, які пристрої (list) отримують які адреси (pool).

Крок 4. Визначити інтерфейси, що є внутрішніми по відношенню до NAT, тобто усі інтерфейси, підключені до внутрішньої мережі.

Крок 5. Визначити інтерфейси, що є зовнішніми відносно NAT, це усі інтерфейси, підключені до зовнішньої мережі.

У таблиці 6.2 приведені команди, необхідні для налаштування динамічного NAT.

Команда ***show ip nat translations*** відображає усі налагоджені статичні перетворення адрес і усі динамічні перетворення, створені в результаті обробки трафіку.

Додавання ключового слова *verbose* виводить додаткову інформацію про кожне перетворення, включаючи час, що пройшов після створення і використання запису.

За умовчанням термін дії записів перетворення збігає через 24 години, якщо налаштування таймерів не було змінене за допомогою команди ***ip nat translation timeout*** *timeout-seconds* в режимі глобальної конфігурації.

Таблиця 6.2 – Послідовність команд для налаштування динамічного NAT

Крок	Дія
1	Визначення пулу глобальних адрес *Router(config)#* ***ip nat pool*** *name start-ip end-ip* {***netmask*** *netmask* | ***prefix-length*** *prefix-length*}
2	Налаштування стандартного списку контролю доступу, що дозволить адреси для перетворення *Router(config)#* ***access-list*** *access-list-number* ***permit*** *source* [*source-wildcard*]
3	Налаштування динамічного перетворення, що пов'язує pool і ACL, визначені на попередніх кроках *Router(config)#* ***ip nat inside source list*** *access-list-number* ***pool*** *name*
4	Увійти в режим налаштування інтерфейсу, до якого підключена внутрішня мережа, та позначити його, як внутрішній *Router(config)#* ***interface*** *type number* *Router(config-if)#* ***ip nat inside***
	Увійти в режим налаштування інтерфейсу, до якого підключена зовнішня мережа, та позначити його, як зовнішній *Router(config)#* ***interface*** *type number* *Router(config-if)#* ***ip nat outside***

Для видалення динамічних записів до закінчення їх часу дії використовують команду привілейованого режиму ***clear ip nat translation***. При проведенні перевірки налаштування NAT рекомендується видаляти динамічні записи. Цю команду можна використати з ключовими словами і змінними, щоб визначити записи, що видаляються. Видалення конкретних записів потрібне для того, щоб не порушити роботу активних сеансів.

Примітка. З таблиці віддаляються тільки динамічні перетворення. Статичні перетворення видалити з таблиці перетворень неможливо.

В якості альтернативи можна скористатися командою ***show running-config*** і знайти команди NAT, ACL, інтерфейсу або пулу з потрібними значеннями.

Налаштування PAT

Залежно від способу виділення публічних IPv4-адрес інтернет-провайдером існують два способи налаштування PAT. У першому випадку інтернет-провайдер виділяє організації декілька публічних IPv4-адрес, а в другому випадку виділяється єдина публічна IPv4-адреса.

Якщо об'єкту було виділено *декілька публічних IPv4-адрес*, то ці адреси можуть бути частиною пулу, використовуваного PAT. Це аналогічно динамічному NAT, за винятком того, що публічних адрес недостатньо для створення взаємно-однозначних відповідностей внутрішніх і зовнішніх адрес. Невеликий пул адрес спільно використовується великим числом пристроїв.

У таблиці 6.3 показані дії з налаштування PAT для використання пулу адрес. Основна відмінність між цим налаштуванням і налаштуванням для динамічного взаємно-однозначного NAT полягає у використанні ключового слова **overload** – воно власне включає PAT.

Таблиця 6.3 – Послідовність команд для налаштування динамічного перетворення PAT з перевантаженням при використанні пулу адрес

Крок	**Дія**
1	Визначення пулу глобальних адрес *Router(config)# **ip nat pool** name start-ip end-ip* {***netmask*** *netmask* | ***prefix-length*** *prefix-length*}
2	Налаштування стандартного списку контролю доступу, що дозволить адреси для перетворення *Router(config)# **access-list** access-list-number **permit** source* [*source-wildcard*]
3	Налаштування перетворення з перевантаженням, що пов'язує pool і ACL, визначені на попередніх кроках *Router(config)# **ip nat inside source list** access-list-number **pool** name **overload***
4	Увійти в режим налаштування інтерфейсу, до якого підключена внутрішня мережа, та позначити його, як внутрішній *Router(config)# **interface** type number* *Router(config-if)# **ip nat inside***
	Увійти в режим налаштування інтерфейсу, до якого підключена зовнішня мережа, та позначити його, як зовнішній *Router(config)# **interface** type number* *Router(config-if)# **ip nat outside***

У таблиці 6.4 показані кроки, необхідні для налаштування PAT з *однією публічною IPv4-адресою*. Якщо доступна тільки одна публічна IPv4-адреса, для налаштування з перевантаженням зазвичай призначається публічна адреса зовнішнього інтерфейсу, що підключається до інтернет-провайдера. Усі внутрішні адреси в пакетах, що виходять із зовнішнього інтерфейсу, перетворюються до цієї IPv4-адреси.

Це налаштування аналогічне динамічному перетворенню PAT з перевантаженням при використанні пулу адрес, за винятком використання ключового слова **interface** замість пулу адрес для визначення зовнішнього IPv4-адреса. Отже, сам пул зовнішніх адрес NAT не визначається.

Процедури роботи PAT з використанням однієї публічної IPv4-адреси наведені на рисунку 6.15.

Таблиця 6.4 – Послідовність команд для налаштування динамічного перетворення PAT з перевантаженням при використанні однієї адреси

Крок	Дія
1	Визначення пулу глобальних адрес *Router(config)#* ***ip nat pool*** *name start-ip end-ip* {***netmask*** *netmask* | ***prefix-length*** *prefix-length*}
2	Налаштування перетворення з перевантаженням, що пов'язує pool і вихідний інтерфейс *Router(config)#* ***ip nat inside source list*** *access-list-number* ***interface*** *type number* ***overload***
3	Увійти в режим налаштування інтерфейсу, до якого підключена внутрішня мережа, та позначити його, як внутрішній *Router(config)#* ***interface*** *type number* *Router(config-if)#* ***ip nat inside***
	Увійти в режим налаштування інтерфейсу, до якого підключена зовнішня мережа, та позначити його, як зовнішній *Router(config)#* ***interface*** *type number* *Router(config-if)#* ***ip nat outside***

Рисунок 6.15 – Процедури роботи PAT з використанням однієї публічної IPv4-адреси

6.2.3. Перенаправлення портів

Перенаправлення портів – це перенаправлення трафіку, адресованого певному порту, від одного вузла мережі на інший вузол. Даний метод дозволяє зовнішнім користувачам зовні досягати порту для приватної IPv4-адреси (в локальній мережі), використовуючи маршрутизатор з підтримкою NAT.

Як правило, для роботи пірінгових програм обміну файлами і виконання таких операцій, як робота веб-сервера або вихідний FTP, потрібно, щоб порти маршрутизатора були перенаправлені або відкриті, як показано на рисунку 6.16. Оскільки NAT приховує внутрішні адреси, пірінгові програми працюють тільки зсередини – в цьому випадку NAT може зіставити вихідні

запити і вхідні відповіді. Тож проблема полягає в тому, що NAT не дозволяє ініціювати запити зовні. Цю ситуацію можна вирішити за допомогою змін, внесених вручну. Можна налаштувати перенаправлення портів, щоб визначити конкретні порти, які можуть бути переадресовані на внутрішні вузли.

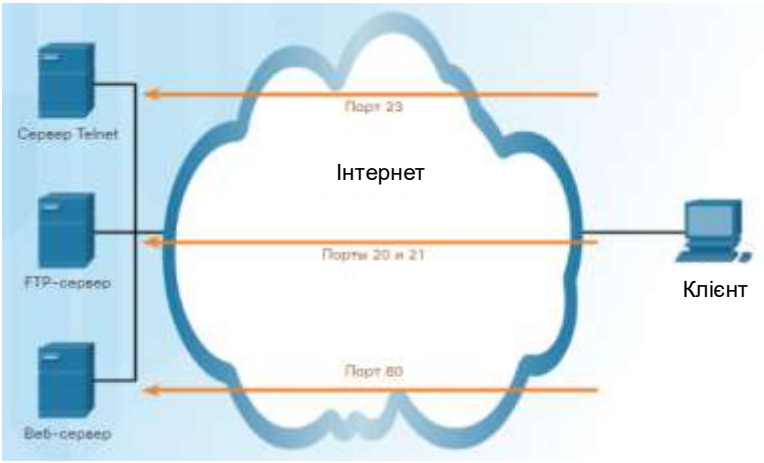


Рисунок 6.16 – Перенаправлення портів

На рисунку 6.17 зображений власник невеликого підприємства, що використовує сервер PoS (пункт продажу) для відстеження продажів і запасів на складі. Сервер доступний всередині складу, і оскільки йому призначена приватна адреса IPv4, публічний доступ до цього сервера з Інтернету неможливий. Включення на локальному маршрутизаторе перенаправлення портів надає власнику доступ до сервера пункту продажів з Інтернету. Перенаправлення портів на маршрутизаторі налаштовується за допомогою номера порту призначення і приватної IPv4-адреси сервера пункту продажів. Для доступу до сервера клієнтська програма повинна використовувати публічну IPv4-адресу маршрутизатора і порту призначення сервера.

Рисунок 6.17 – Використання перенаправлення портів

Якщо використовуваний номер порту відрізняється від стандартного порту призначення, який формується конкретним додатком, то його можна

додати до URL-адреси (IPv4-адреси), відокремивши двокрапкою (:). Наприклад, якщо веб-сервер прослуховує порт 8080, користувач повинен ввести **http://www.example.com:8080 (або http: // 209.16.17.2:15555)** .

На рисунку 6.18 показано вікно настройки перенаправлення на один порт для маршрутизатора бездротового зв'язку Linksys. За замовчуванням перенаправлення портів на маршрутизаторі не включене.

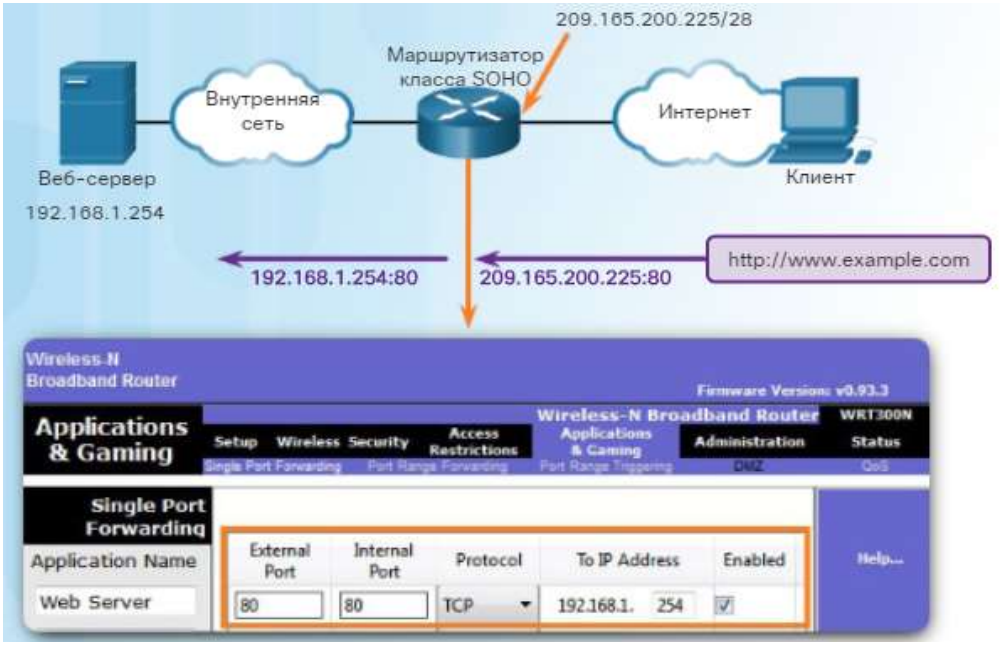


Рисунок 6.18 – Вікно налаштування перенаправлення на один порт для маршрутизатора бездротового зв'язку Linksys

Перенаправлення портів для додатків можна включити, вказавши внутрішню локальну адресу, на яку повинні перенаправлятися запити. На рисунку 6.18 запити до служби HTTP, що надходять на маршрутизатор бездротового зв'язку, перенаправляються на веб-сервер з внутрішньою локальною адресою 192.168.1.254. Якщо зовнішній WAN IPv4-адрес маршрутизатора бездротового зв'язку – 209.165.200.225, то зовнішній користувач може ввести **http://www.example.com**, і цей маршрутизатор перенаправить запит HTTP внутрішньому веб-серверу за IPv4-адресою 192.168.1.254, використовуючи номер порту за замовчуванням – 80.

Можна також вказати номер порту, що відрізняється від номера порту за замовчуванням, відповідного 80. Однак зовнішній користувач повинен знати конкретний використовуваний номер порту. Щоб визначити інший порт, необхідно змінити значення зовнішнього порту (External Port) у вікні перенаправлення на один порт (Single Port Forwarding).

Реалізація перенаправлення портів за допомогою команд IOS аналогічна застосуванню команд настройки статичного NAT. Перенаправлення портів фактично є статичним перетворенням NAT із зазначеним номером порту TCP або UDP.

У таблиці 6.4 розкриті складові команди статичного NAT, що забезпечує настройку перенаправлення портів за допомогою IOS:

Router(config)# ***ip nat inside source static*** {***tcp***|***udp*** *local-ip local-port global-ip global- port*} [**extendable**]

Таблиця 6.5 – Налаштування перенаправлення портів в Cisco IOS

Параметр	Опис
tcp або ***udp***	Вказує тип порту, що буде використаний TCP або UDP
local-ip	IPv4-адреса, призначена вузлу внутрішньої мережі, як правило з діапазону приватних адрес (RFC 1918)
local-port	Локальний порт TCP / UDP в діапазоні від 1 до 65535 до якого сервер очікує підключення
global-ip	Унікальна глобальна IPv4-адреса, яку зовнішні клієнти будуть використовувати для підключення до серверу
global- port	Глобальний порт TCP / UDP в діапазоні від 1 до 65535, який зовнішні клієнти будуть використовувати для підключення до серверу
extendable	Функція, що дозволяє налаштувати певні неоднозначні статичні перетворення, які дозволять за необхідності розширити перетворення до кількох портів

На рисунку 6.19 наведено приклад налаштування перенаправлення портів за допомогою команд IOS на маршрутизаторі R2. 192.168.10.254 – це внутрішня локальна IPv4-адреса веб-сервера, що прослуховує порт 80. Користувачі отримають доступ до цього внутрішнього веб-сервера за допомогою глобальної IPv4-адреси 209.165.200.225, яка є глобальною унікальною загальнодоступною IPv4-адресою. В даному випадку це адреса інтерфейсу Serial 0/1/0 маршрутизатора R2. В якості глобального порту налаштований порт 8080. Він буде портом призначення, що використовується разом з глобальною IPv4-адресою 209.165.200.225 для доступу до внутрішнього веб-сервера. У налаштуванні такого NAT використані наступні параметри команди:

- *local-ip* = 192.168.10.254
- *local-port* = 80
- *global-ip* = 209.165.200.225
- *global-port* = 8080

Якщо не використовується стандартний номер порту, що притаманний додатку (наприклад, для web-браузера це порти 80 або 8080), то клієнт має вказати номер порту в додатку.

Як і для інших типів NAT, для перенаправлення портів необхідно налаштувати як внутрішній, так і зовнішній інтерфейси NAT.

Аналогічно статичному NAT, для перевірки перенаправлення портів можна використовувати команду **show ip nat translations** , як показано на рисунку 6.20.

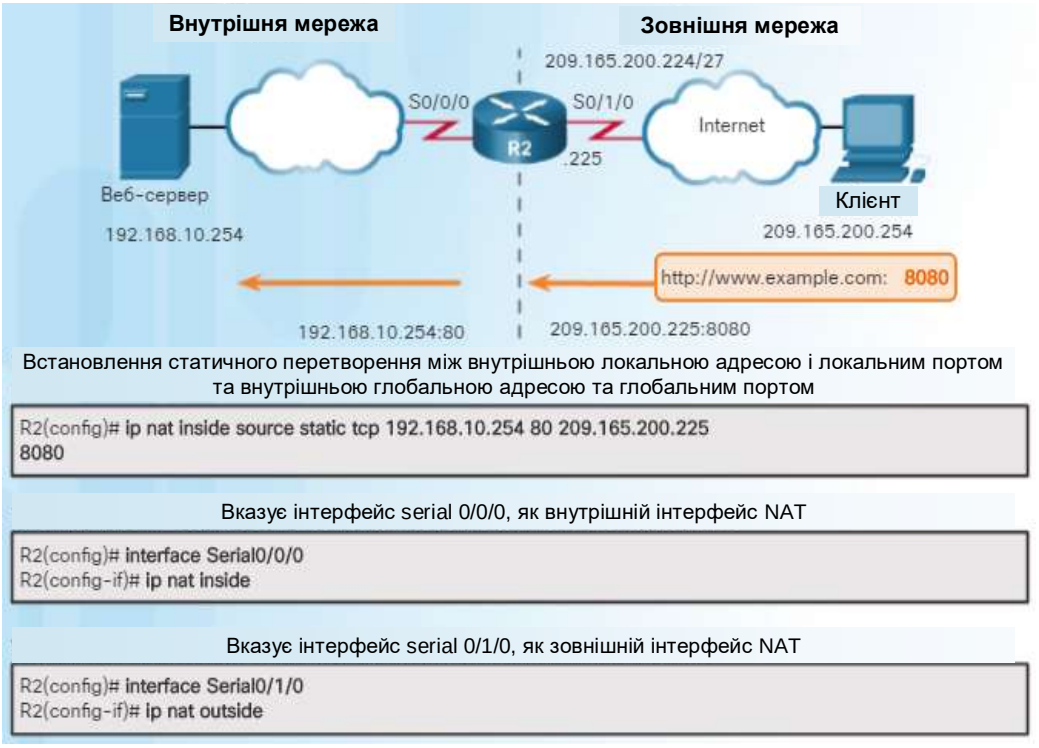


Рисунок 6.19 – Приклад налаштування перенаправлення портів за допомогою команд IOS

У розглянутому прикладі, коли маршрутизатор отримує пакет з внутрішньою глобальною IPv4-адресою 209.165.200.225 і TCP-портом призначення 8080, він виконує пошук в таблиці NAT, використовуючи в якості ключа IPv4-адрес призначення і порт призначення. Потім маршрутизатор перетворює адресу у внутрішню локальну адресу вузла 192.168.10.254 і порт призначення 80. Потім R2 пересилає пакет веб-сервера. Для зворотних пакетів, що йдуть від веб-сервера до клієнта, цей процес інвертується.

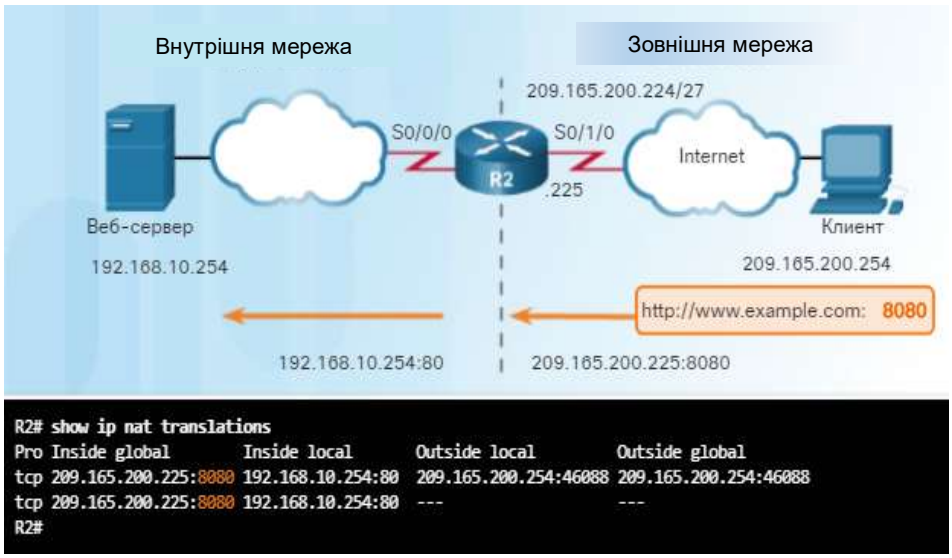


Рисунок 6.20 – Використання команди **show ip nat translations** для перевірки перенаправлення портів

Контрольні питання до розділу 6

1. Дайте визначення списків контролю доступу – ACL та перерахуйте завдання, що вони виконують.

2. Охарактеризуйте статичний механізм перетворення адрес NAT.

3. Наведіть формат команд та порядок налаштування стандартного ACL-списку.

4. Наведіть формат команд та поясніть порядок налаштування перенаправлення портів в пристроях Cisco IOS.

5. Наведіть та поясніть формат команд для застосування перетворень адрес на інтерфейсах, а також для перевірки статистики їх роботи.

РОЗДІЛ 7
АУТЕНТИФІКАЦІЯ, АВТОРИЗАЦІЯ ТА ОБЛІК ДІЯЛЬНОСТІ АДМІНІСТРАТОРІВ МЕРЕЖ

7.1. Організація процедур аутентифікації, авторизації та обліку діяльності адміністраторів мереж

7.1.1. Властивості та принципи роботи процедур AAA

Мережа повинна бути спроектована так, щоб була можливість контролювати, кому і коли дозволено до неї підключатися і що їм дозволено в ній робити. Ці особливості проекту мережі визначені в політиці мережної безпеки. Політика визначає доступ до мережних ресурсів мережних адміністраторів, корпоративних користувачів, віддалених користувачів, ділових партнерів і клієнтів. Політика мережної безпеки також може визначати систему звітності, де реєструється, хто і коли входив в мережу і що вони в ній робив.

Система управління доступом до мережі з використанням тільки користувальницького режиму або тільки команд паролів привілейованого режиму обмежена і не дуже добре масштабується. Використання протоколу автентифікації, авторизації та обліку (AAA) створює необхідну структуру для масштабованої захисту доступу.

Маршрутизатор і комутатори Cisco IOS можна налаштувати так, щоб вони використовували AAA для доступу до локальної базі даних імен користувачів і паролів. Використання локальної бази даних імен користувачів і паролів забезпечує більш високий рівень захисту, ніж простий пароль. Це економічне і легко реалізоване рішення безпеки для невеликих організацій.

Система управління захищеним доступом Cisco (Access Control System, ACS)

Великим організаціям потрібні більш масштабні рішення з автентифікації. Маршрутизатор і комутатори Cisco IOS можна налаштувати так, щоб вони використовували AAA для аутентифікації в системі *Cisco Secure Access Control System (ACS)*. Система управління доступом Cisco Secure Access Control System (ACS) – це централізоване рішення, що об’єднує політику доступу до мережі і політику ідентифікації, застосовувані в організації.

Cisco ACS добре масштабується, тому що всі інфраструктурні пристрої мають доступ до центрального серверу. Рішення Cisco Secure ACS також відрізняється стійкістю до відмов, тому що дозволяє налаштовувати кілька серверів.

У сімейство Cisco ACS входять масштабовані високопродуктивні сервери контролю доступу. Їх можна використовувати для управління доступом адміністраторів і налаштування всіх мережних пристроїв.

Інтеграція AAA з Active Directory

Microsoft Active Directory (AD) – це служба каталогів для доменних мереж Windows, що входить в склад більшості операційних систем сімейства Windows Server. Контролер домену AD використовується для примусового впровадження політик безпеки за допомогою автентифікації та авторизації користувачів при їх вході в домен Windows. Microsoft AD також можна використовувати для обробки автентифікації і авторизації на пристроях Cisco IOS.

Хоча Cisco Secure ACS можна інтегрувати для використання служби AD, Microsoft Windows Server також можна налаштувати як сервер AAA. Реалізація сервера AAA компанії Microsoft з використанням протоколу RADIUS називається службою аутентифікації Інтернету (IAS). Починаючи з версії Windows Server 2008, служба IAS перейменована в сервер мережних політик (NPS).

Для Cisco IOS використовується точно така ж конфігурація, як і для зв'язку з будь-яким сервером RADIUS. Єдина відмінність полягає в тому, що для виконання аутентифікації і авторизації використовується контролер AD сервера Microsoft.

Інтеграція AAA і Identity Service Engine

Щоб забезпечити доступ до корпоративних сервісів тільки уповноваженим особам, тільки з дозволених пристроїв, Cisco пропонує рішення Cisco Identify Services Engine (ISE). ISE надає інформацію про користувачів і пристрої, які здійснюють доступ до мережі. Це рішення нового покоління не тільки підтримує модель AAA, але також примусово вводить політики безпеки і доступу на кінцевих пристроях, що підключаються до комутаторів і маршрутизаторів організації. Воно спрощує управління різноманітними пристроями і підтримує такі функції, як профілювання пристроїв, оцінка стану, управління гостьовим доступом і доступ до мережі на базі ідентифікації.

Cisco Identity Services Engine (ISE) – це платформа політик ідентифікації і контролю доступу, яка допомагає організаціям забезпечити відповідність нормативним вимогам, підвищити безпеку інфраструктури та прискорити роботу служб. Архітектура Cisco ISE дозволяє організаціям збирати контекстну інформацію в реальному часі у мереж, користувачів і пристроїв. Адміністратор може використовувати цю інформацію для завчасного прийняття управлінських рішень з прив'язкою ідентифікації до різних елементів мережі. У число цих елементів мережі входять комутатори доступу, контролери бездротових мереж (WLC), VPN, шлюзи і комутатори центру обробки даних.

Концепція використання на роботі власних пристроїв (BYOD) стає поширеною і навіть необхідною у багатьох організаціях. Cisco ISE визначає справедливі політики доступу і забезпечує відповідність нормативним вимогам всіх пристроїв, включаючи власні пристрої кінцевих користувачів.

Cisco ISE – це основний компонент політик Cisco TrustSec, що захищає від несанкціонованого доступу такі ресурси, як дані, додатки і мобільні

пристрої. Cisco ISE об’єднує визначення політик, контроль і звітність в одному пристрої. ISE використовує існуючу мережну інфраструктуру для надання мережним адміністраторам інформації про підключаються до мережі кінцевих пристроях.

Набір інструментів ISE має чотири характеристики:

– ***Профілювання пристроїв.*** Може використовуватися, щоб визначити, персональне цей пристрій або корпоративне.

– ***Оцінка стану.*** Визначає, чи є на пристрої віруси або підозрілі програми, перш ніж воно отримає доступ в мережу. Оцінка стану також дозволяє визначити необхідність оновлення програмного забезпечення пристрою.

– ***Управління гостями.*** Надання тимчасового гостьового доступу і застосування відповідних обмежень.

– ***AAA.*** Об’єднує автентифікацію, авторизацію і облік в одному пристрої з можливостями профілювання пристроїв, оцінки стану і управління гостями.

Основна функція ISE – надання доступу до мережі на основі ідентифікації. ISE підтримує управління ідентифікацією з контекстної інформацією:

– Щоб визначити, які користувачі отримують доступ до мережі на авторизованому пристрої, відповідному політикам.

– Щоб ідентифікувати користувача, місце розташування і історію доступу, що можна використовувати для забезпечення сумісності і звітності.

– Щоб призначати служби в залежності від призначеної ролі користувача, групи і відповідної політики (посада, розташування, тип пристрою і т.д.).

– Щоб надавати пройшли автентифікацію користувачам доступ до певних сегментах мережі або певних додатків і послуг в відповідності з результатами автентифікації.

Автентифікація без AAA

Найпростіший метод автентифікації для віддаленого доступу – налаштувати ім’я користувача та пароль на консолі, лініях vty і допоміжних портах, як показано на рисунку 7.1. Цей метод найпростіший в реалізації, але при цьому також найслабший і найменш безпечний. Цей метод не дає можливості обліку. Будь-який користувач з паролем може отримати доступ до пристрою і змінити конфігурацію. Хоча Telnet можна налаштувати з використанням імені користувача та пароля, але повідомлення відправляються в форматі звичайного тексту, тобто імена та паролі можуть бути перехоплені і використані.

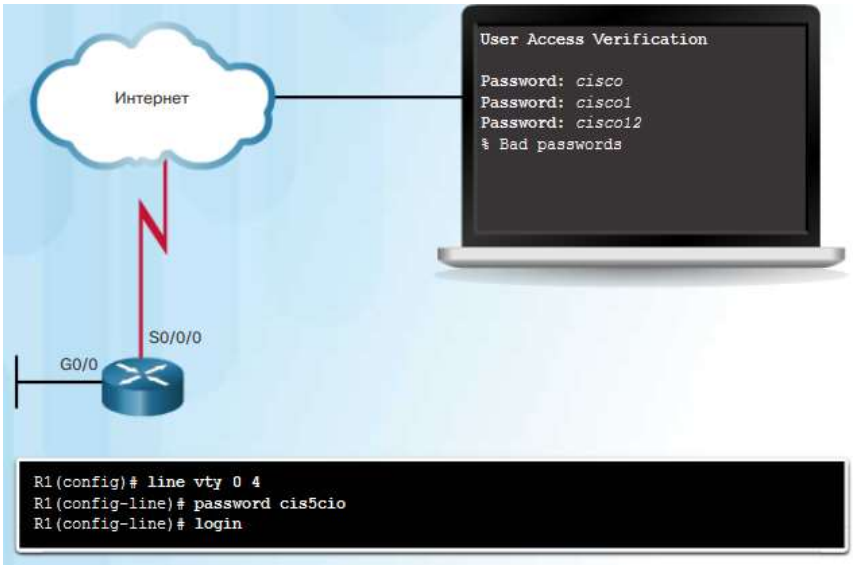


Рисунок 7.1 – Метод автентифікації для віддаленого доступу

SSH – більш безпечна форма віддаленого доступу. Вона вимагає введення імені користувача і пароля, які передаються в зашифрованому вигляді. Метод локальної бази даних забезпечує додаткову безпеку, тому що атакуючий повинен знати ім'я користувача і пароль. Також він забезпечує певні можливості обліку, оскільки ім'я користувача реєструється при вході користувача в систему.

Компоненти AAA

Служби безпеки мережі AAA забезпечують базову інфраструктуру настройки контролю доступу на мережні пристрої. Система мережної та адміністративної безпеки AAA в середовищі Cisco має три функціональних компоненти:

– **Автентифікація** – дозволяє контролювати, кому дозволено доступ до мережі. Користувачі і адміністратори повинні довести, що вони – саме ті, за кого себе видають. Автентифікація проводиться за допомогою перевірки комбінацій імені користувача і пароля, контрольних питань і відповідей, токен-карт і інших методів. *Наприклад: "Я користувач student і я знаю пароль, який доводить це"* .

– **Авторизація** – дозволяє контролювати, що автентифікованим користувачам дозволено робити. Служби авторизації визначають, до яких ресурсів користувач може отримувати доступ і які операції він має право виконувати. *Приклад: "Користувач student може отримувати доступ до хост-серверу XYZ тільки з допомогою SSH"*.

– **Облік і аудит** – система перевіряє виконані дії при доступі до мережі, облікує дії користувача, включаючи ресурси, до яких він отримав доступ, тривалість доступу до конкретного ресурсу і будь-які внесені ним зміни. Система обліку відстежує спосіб використання мережних ресурсів. *Приклад: "Користувач student мав доступ до хост-серверу XYZ з допомогою SSH протягом 15 хвилин"*.

Дана концепція аналогічна використанню кредитної картки. Кредитна карта визначає, хто може її використовувати, скільки цей користувач може витратити, а також враховує покупки товарів і послуг користувачем.

Cisco надає два стандартних методи реалізації сервісів AAA:

– **Локальна автентифікація AAA** – використовує для автентифікації базу даних, збережену в самому пристрої (рисунок 7.2) . Це та ж база даних, яка необхідна для установки CLI на основі ролей. Локальна система AAA ідеально підходить для невеликих мереж.

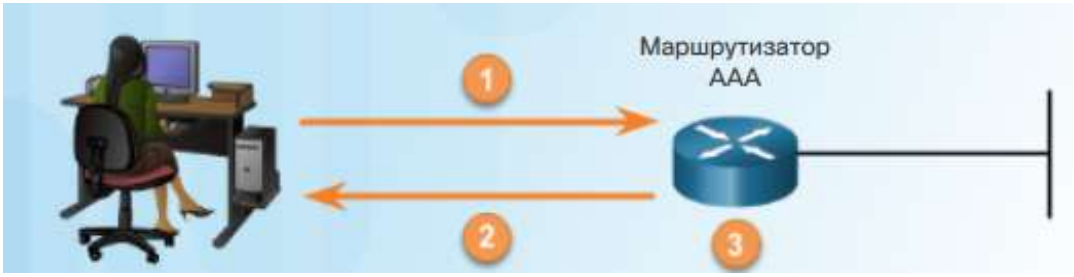


Рисунок 7.2 – Локальна автентифікація AAA

Метод локальної бази даних має певні обмеження. Облікові записи користувачів необхідно локально налаштовувати на кожному пристрої. У великої корпоративної інфраструктурі з великим числом маршрутизаторів і комутаторів розгортання і зміна локальних баз даних на кожному пристрої може забирати багато часу. Крім того, локальна конфігурація бази даних не підтримує повернення до попередньої версії бази (відкат) автентифікації. Отже, якщо адміністратор втратив ім'я користувача і пароль для пристрою, то без резервного копіювання даних автентифікації єдиним варіантом стає відновлення пароля, що призводить до втрати конфігурації пристрою.

Краще рішення полягає в тому, щоб всі пристрої використовували одну і ту ж базу даних імен користувача і паролів з центрального сервера.

– **Серверна аутентифікація AAA** – у разі реалізації на базі сервера маршрутизатор взаємодіє з сервером AAA, наприклад Cisco Secure Access Control System (ACS) для Windows, як показано на рисунку 7.3. Центральний сервер AAA містить імена користувачів і паролі для всіх користувачів. Маршрутизатор використовує для зв'язку з сервером AAA службу віддаленої аутентифікації користувачів з комутованим доступом ***(RADIUS, Remote Authentication Dial-In User)*** або протокол управління доступом до контролера термінального доступу ***(TACACS+, Terminal Access Controller Access Control System)***. Серверний варіант AAA більш підходить при наявності значної кількості маршрутизаторів і комутаторів.

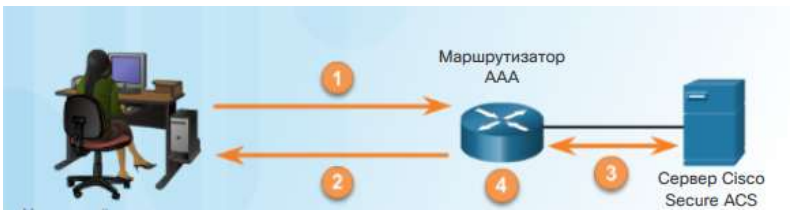


Рисунок 7.3 – Серверна аутентифікація AAA

7.1.2. Робота процедур AAA через локальний список користувачів

При реалізації процедур AAA через локальний список користувачів виконується локальне збереження імен користувачів і паролів маршрутизатора Cisco, а *автентифікація* користувачів проводиться за цією локальною базою даних. Цей метод іноді називається самодостатньою автентифікацією.

Після успішної автентифікації користувачів з локальним джерелом даних AAA вони автоматично авторизуються для доступу до певних мережних ресурсів. *Авторизація* визначає, що користувачі можуть або не можуть робити в мережі після автентифікації. З точки зору адміністрування пристроїв, у випадку локальної автентифікації рівні привілеїв і командний рядок (CLI) на основі ролей дають користувачам певні права та привілеї при виконанні певних команд на маршрутизаторі.

Авторизація зазвичай реалізується з допомогою серверного рішення AAA. Авторизація використовує створений набір атрибутів, що описують доступ користувача до мережі. Ці атрибути порівнюються з інформацією, що міститься в базі даних AAA, використовуються для визначення обмежень цього користувача і відправляються на локальний маршрутизатор, до якого підключений користувач.

Авторизація проводиться автоматично і не вимагає від користувачів додаткових дій після автентифікації. Авторизація виконується відразу ж після автентифікації користувача.

Облік AAA здійснює збір інформації по використанню мережі і формує звіти. Дані можуть збиратися в інтересах аудиту або білінгу. Зібрані дані можуть включати час початку і зупинки підключення, виконані команди, число пакетів і число байт.

Облік реалізується виключно з допомогою серверного рішення AAA. Дана служба повідомляє серверу ACS статистику використання. Цю статистику можна витягти для створення докладних звітів про зміни конфігурації мережі.

Облік часто поєднується з автентифікацією AAA. Це допомагає адміністративному персоналу мережі управляти доступом до мережних пристроїв. Облік забезпечує більш високий рівень безпеки, ніж проста автентифікація. На серверах AAA ведеться детальний журнал дій користувачів, які здійснили автентифікацію на пристрої. Зокрема, в журналі реєструються всі відправлені користувачем команди EXEC і зміни конфігурації. У журналі міститься безліч полів даних, включаючи ім’я користувача, дату і час і фактично введену користувачем команду. Ця інформація корисна при діагностиці та усуненні несправностей пристроїв. Також вона забезпечує захист від осіб, які виконують шкідливі дії.

Налаштування локальної AAA

Локальну автентифікацію AAA слід налаштовувати для невеликих мереж. Цей метод використовує локальні імена користувачів і паролі,

збережені на маршрутизаторі. Системний адміністратор повинен заповнити локальну базу даних безпеки, ввівши профілі з іменами користувачів і паролями для кожного користувача, який може увійти в систему. Метод локальної автентифікації AAA схожий з використанням команди **login local**, за винятком, що AAA також дає можливість налаштувати резервні методи автентифікації.

Щоб налаштувати локальні сервіси AAA для автентифікації доступу адміністратора, потрібно ряд простих кроків (рисунок 7.4):

Крок 1. Додати імена користувачів і паролі в локальну базу даних маршрутизатора для користувачів, яким необхідний адміністративний доступ до цього маршрутизатора.

Крок 2. Включити AAA в глобальному режимі на маршрутизаторі.

Крок 3. Налаштувати параметри AAA на маршрутизаторі.

Крок 4. Підтвердити конфігурацію AAA і усунути несправності.

Щоб включити AAA, потрібно попередньо виконати команду глобальної конфігурації **aaa new-model**. Щоб відключити AAA, потрібно використовувати форму **no** цієї ж команди.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default local-case enable
R1(config)# aaa authentication login SSH-LOGIN local-case
R1(config)# line vty 0 4
R1(config-line)# login authentication SSH-LOGIN
```

Рисунок 7.4 – Приклад налаштування локальної AAA

Примітка. До введення цієї команди ніякі інші команди AAA не доступні. Коли команда **aaa new-model** вводиться в перший раз, аутентифікація по замовчуванням автоматично виробляється для всіх ліній, крім консолі, з використанням локальної бази даних. За цієї причини перед активацією AAA завжди необхідно налаштовувати запис в локальній базі даних.

7.1.3. Робота процедур AAA через віддаленій сервер

У більшості корпоративних середовищ використовується безліч маршрутизаторів, комутаторів та інших інфраструктурних пристроїв Cisco, у маршрутизаторів є безліч адміністраторів, а доступ до корпоративної мережі потрібен сотням або тисячам користувачів. Обслуговування локальної бази даних для кожного пристрою в мережі такого масштабу недоцільно.

Щоб вирішити цю проблему, можна використовувати для управління доступом користувачів і адміністраторів до всієї корпоративної мережі з допомогою одного або декількох серверів AAA, наприклад Cisco Secure ACS. Cisco Secure ACS може створювати централізовану базу даних користувачів і адміністративного доступу, якої зможуть користуватися всі пристрої мережі. Також підтримується робота з багатьма зовнішніми базами даних, в тому

числі на базі Active Directory і Lightweight Directory Access Protocol (LDAP). У цих базах даних зберігаються дані облікових записів користувачів і паролі, що дозволяє централізовано адмініструвати облікові записи користувачів. Для додаткового резервування можна використовувати кілька серверів.

Взаємодія між мережевим пристроєм, доступ до якого визначається процедурою AAA, та відповідним сервером здійснюється за одним з протоколів – RADIUS або TACACS +.

TACACS+ (*Terminal Access Controller Access Control System*) і RADIUS (*Remote Authentication Dial-In User*) – два основні протоколи, які використовуються в пристроях безпеки, маршрутизаторах і комутаторах Cisco для зв'язку з серверами AAA. Як представлено в таблиці 7.1, кожен з протоколів підтримує різні функції і можливості. Вибір між TACACS + і RADIUS залежить від потреб організації.

Таблиця 7.1 – Порівняльна характеристика TACACS+ і RADIUS

	TACACS+	**RADIUS**
Функціональні можливості	Розділяє AAA відповідно до архітектури AAA, що забезпечує модульний принцип реалізації сервера безпеки	Об'єднує автентифікацію і авторизацію, але відокремлює облік
Стандарт	Зазвичай підтримується компанією Cisco	Відкритий стандарт / стандарт RFC
Транспортний протокол	TCP	UDP
CHAP	Двохнаправлений запит і відповідь, що використовуються в протоколі Challenge Handshake Authentication Protocol (CHAP)	Односпрямований запит і відповідь з сервера безпеки RADIUS в клієнт RADIUS
Конфіденційність	Шифрується весь пакет	Шифрується пароль
Персоналізація	Забезпечує авторизацію команд маршрутизатора для кожного користувача або для кожної групи	Не дозволяє виконувати авторизацію команд маршрутизатора для кожного користувача або для кожної групи
Облік	З обмеженнями	Розширений

Три основних характеристики TACACS +:

- розділяє автентифікацію і авторизацію;
- шифрує всі дані;
- використовує TCP-порт 49.

Чотири основних характеристики RADIUS:

– об’єднує автентифікацію і авторизацію RADIUS в рамках одного процесу;

– шифрує тільки пароль;

– використовує UDP;

– підтримує технології віддаленого доступу 802.1X і протокол ініціювання сеансу (SIP, Session Initiation Protocol).

Наприклад, великий інтернет-провайдер може вибрати RADIUS, тому що він підтримує детальний облік, необхідний для білінгу користувачів. Організація з різними групами користувачів може вибрати TACACS+, тому що він вимагає застосування політик авторизації на рівні користувачів або груп.

Хоча для взаємодії між маршрутизатором і серверами AAA може використовуватися будь-який з протоколів, протокол TACACS+ вважається більш захищеним. Це пов’язано з тим, що всі передані по протоколу TACACS+ дані шифруються, а при передачі по протоколу RADIUS шифрується тільки пароль користувача. RADIUS не шифрується імена користувачів, облікову інформацію та іншу інформацію, передану в повідомленнях RADIUS.

Автентифікація TACACS+

TACACS + підтримується маршрутизаторами і серверами доступу Cisco (рисунок 7.5). TACACS+ забезпечує окремі сервіси AAA. Відділення сервісів AAA дає гнучкість реалізації, дозволяючи використовувати протокол TACACS+ для авторизації і обліку і при цьому використовувати інший метод автентифікації.

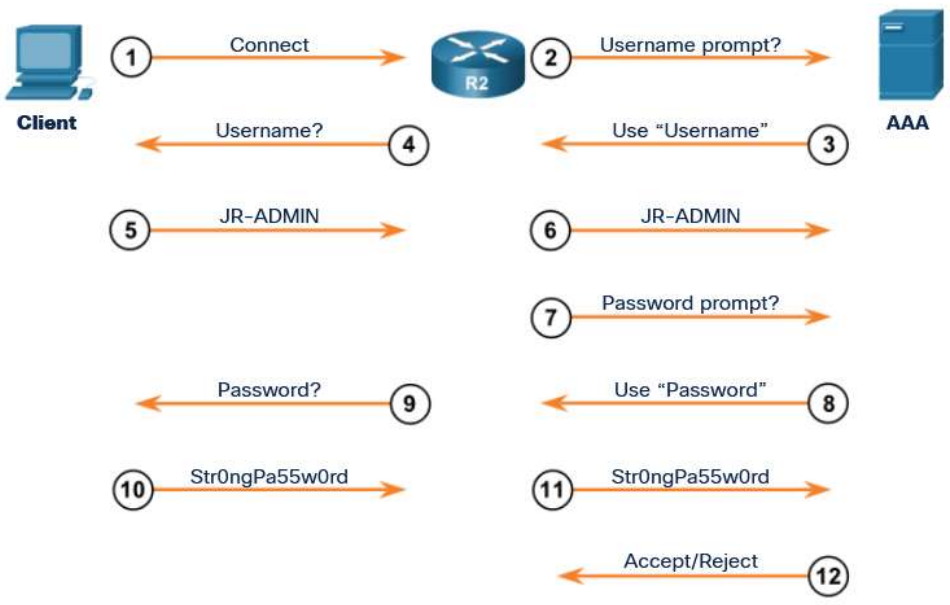


Рисунок 7.5 – Процес автентифікації TACACS+

Розширення протоколу TACACS+ дають додаткові типи запитів автентифікації і кодів відповідей по порівнянні з вихідною специфікацією

TACACS. TACACS+ забезпечує підтримку різноманітних протоколів, включаючи IP і застарілий протокол AppleTalk. У звичайних операціях TACACS+ для найбільшої безпеки зв'язку шифрується все тіло пакета і використовується порт TCP 49.

Автентифікація RADIUS

Протокол RADIUS приховує паролі при передачі навіть з протоколом автентифікації по паролю (PAP). Для цього використовується досить складна операція, що включає змішування дайджесту повідомлень 5 (MD5) і загальний секрет. Однак інша частина пакета передається в простому текстовому форматі.

RADIUS (рисунок 7.6) об'єднує автентифікацію і авторизацію в один процес. При автентифікації користувача здійснюється і його авторизація. RADIUS використовує порт UDP 1 645 або 1812 для автентифікації і порт UDP 1646 або 1813 для обліку.

RADIUS широко використовується постачальниками послуг VoIP. Він передає облікові дані кінцевих пристроїв SIP, наприклад широкосмугових телефонів, в реєстр SIP з допомогою автентифікації дайджесту, а потім на сервер RADIUS з допомогою RADIUS. Протокол автентифікації RADIUS зазвичай також використовується в стандарті безпеки 802.1X.

Примітка. Протокол DIAMETER – це протокол AAA нового покоління, який є альтернативою RADIUS. DIAMETER – це стандарт IETF, який використовує новий транспортний протокол, який називається протоколом передачі управління потоком (SCTP), і TCP замість UDP.

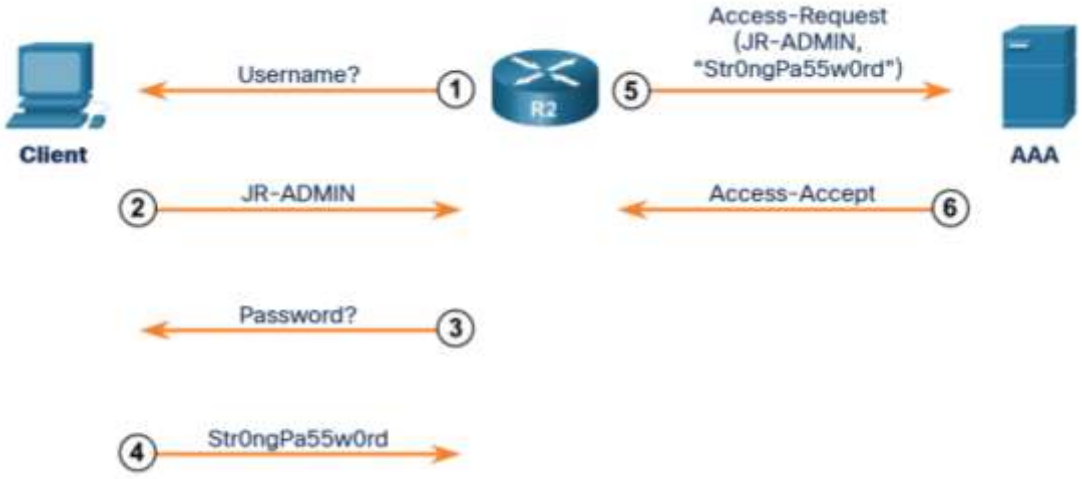


Рисунок 7.6 – Процес автентифікації RADIUS

Інтеграція TACACS + і ACS

Cisco Secure ACS для Windows Server – це рішення, що забезпечує сервіси AAA для TACACS+ і RADIUS. Cisco Secure ACS версії 5.6 – складна платформа контролю доступу на основі політик. У число характеристик Cisco Secure ACS входять:

– розподілена архітектура для розгортання в системах середнього і великого масштабу;

– компактний веб-інтерфейс з інтуїтивно зрозумілою навігацією, доступний клієнтам IPv4 і IPv6;

– автентифікація адміністратора через Microsoft Active Directory і Lightweight Directory Access Protocol (LDAP);

– автоматична відправка звітів по розкладом на адресу електронної пошти;

– інтегровані можливості розширеного моніторингу, звітності та діагностики для забезпечення контролю і прозорості даних по стану Cisco Secure ACS з допомогою пасток SNMP;

– шифровані (захищені) системні журнали;

– гнучке деталізоване адміністрування пристроїв в мережах IPv4 і IPv6 з повними можливостями аудиту і звітності, необхідними для дотримання стандартів.

Процедура налаштування серверної автентифікації AAA

На відміну від локальної автентифікації AAA, серверна автентифікація AAA вимагає визначення різних серверів TACACS+ і RADIUS, до яких служба AAA повинна звертатися при автентифікації і авторизації користувачів.

Процедура настройки серверної автентифікації складається з чотирьох кроків:

Крок 1. Для використання всіх елементів AAA необхідно включити AAA в глобальному режимі.

Крок 2. Вказати сервер Cisco Secure ACS, який буде надавати маршрутизатора послуги AAA. Це може бути сервер TACACS + або RADIUS.

Крок 3. Настроїти ключ шифрування, необхідний для шифрування передачі даних між сервером доступу до мережі і Cisco Secure ACS.

Крок 4. Настроїти список методів аутентифікації AAA для використання сервера TACACS + або RADIUS. Для цілей резервування можна налаштувати декілька серверів.

На рисунку 7.7 наведені приклади команд для налаштування серверів TACACS+ і RADIUS та команда впровадження серверної автентифікації. Можливі варіанти команди автентифікації наведені на рисунку 7.8.

Серверна авторизація AAA

Автентифікація забезпечує перевірку законності доступу пристрою або кінцевого користувача, а авторизація дозволяє або забороняє користувачам отримувати доступ до певних зон або програмами мережі.

Протокол TACACS+ дозволяє відокремлення автентифікації від авторизації. Маршрутизатор можна налаштувати так, щоб після успішної автентифікації користувач міг виконувати тільки певні функції. Необхідно пам’ятати, що RADIUS не відокремлює автентифікацію від авторизації.

```
R1(config)# aaa new-model
R1(config)#
R1(config)# tacacs server Server-T
R1(config-server-tacacs)# address ipv4 192.168.1.100
R1(config-server-tacacs)# single-connection
R1(config-server-tacacs)# key TACACS-Pa55w0rd
R1(config-server-tacacs)# exit
R1(config)#
R1(config)# radius server SERVER-R
R1(config-radius-server)# address ipv4 192.168.1.101 auth-port 1812 acct-port 1813
R1(config-radius-server)# key RADIUS-Pa55w0rd
R1(config-radius-server)# exit
R1(config)#
R1(config)# aaa authentication login default group tacacs+ group radius local-case
```

Рисунок 7.7 – Серверна автентифікація

```
R1(config)# aaa authentication login default ?
  cache          Use Cached-group
  enable         Use enable password for authentication.
  group          Use Server-group
  krb5           Use Kerberos 5 authentication.
  krb5-telnet    Allow logins only if already authenticated via Kerberos V
                 Telnet.
  line           Use line password for authentication.
  local          Use local username authentication.
  local-case     Use case-sensitive local username authentication.
  none           NO authentication.
  passwd-expiry  enable the login list to provide password aging support

R1(config)# aaa authentication login default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Рисунок 7.8 – Приклади команд серверної автентифікації

Інший важливий аспект авторизації – можливість контролювати доступ користувача до певних послуг. Контроль доступу до командам конфігурації значно спрощує захист інфраструктури в великих корпоративних мережах. Дозволи окремих користувачів Cisco Secure ACS спрощують настройку конфігурації мережних пристроїв.

На рисунку 7.9 показаний приклад команд для налаштування серверної авторизації, а на рисунку 7.10 можливі варіанти такого налаштування.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
```

Рисунок 7.9 – Серверна авторизація

```
Router(config)# aaa authorization (network | exec | commands level) {default | list-name}
method1… [method4]
```

```
R1(config)# aaa authorization exec ?
  WORD Named authorization list.
  default The default authorization list.
```

```
R1(config)# aaa authorization exec default ?
  cache              Use Cached-group
  group              Use server-group.
  if-authenticated   Succeed if user has authenticated.
  krb5-instance      Use Kerberos instance privilege maps.
  local              Use local database.
  none               No authorization (always succeeds).

R1(config)# aaa authorization exec default group ?
  WORD     Server-group name
  ldap     Use list of all LDAP hosts.
  radius   Use list of all Radius hosts.
  tacacs+  Use list of all Tacacs+ hosts.
```

Рисунок 7.10 – Варіанти команд серверної авторизації

Серверний облік AAA

Компаніям часто потрібно стежити за тим, які ресурси використовують окремі користувачі або групи. Облік AAA дозволяє здійснювати контроль за використанням ресурсів. Наприклад, це потрібно, коли один відділ стягує з іншого відділу плату за доступ або коли одна компанія надає внутрішню підтримку іншої компанії.

Хоча облік зазвичай вважається завданням управління мережею або фінансового управління, але він тісно пов'язаний з безпекою. Зокрема, система обліку створює список користувачів з зазначенням часу їх входу в систему. Наприклад, якщо адміністратор дізнається, що співробітник увійшов в систему посеред ночі, ця інформація може стати приводом для подальшого розслідування причин такого входу.

Ще одна причина впровадження обліку – створення списку змін в мережі з зазначенням користувача, який вносить зміни, і точного характеру цих змін. Ця інформація допомагає в діагностиці та усуненні несправностей, якщо зміни тягнуть за собою непередбачені результати.

Cisco Secure ACS виступає в якості центрального сховища облікової інформації. ACS відстежує події в мережі приблизно так само, як банк відстежує операції по кредитній карті. Дані при кожному сеансі підключення через Cisco Secure ACS повністю фіксуються і зберігаються на сервері. Ця збережена інформація може виявитися дуже корисною для управління, аудиту безпеки, планування ресурсів і білінгу за використання мережі.

Як і в випадку аутентифікації і авторизації, списки методів обліку визначають конкретні способи виконання обліку і послідовність їх застосування. Після активації список методів обліку по замовчуванням

автоматично застосовується до всіх інтерфейсах, крім тих, для яких явно визначено користувальницький список методів обліку.

На рисунку 7.11 показаний приклад команд для налаштування серверного обліку, а на рисунку 7.12 можливі варіанти такого налаштування.

```
R1(config)# username JR-ADMIN algorithm-type scrypt secret Str0ng5rPa5w0rd
R1(config)# username ADMIN algorithm-type scrypt secret Str0ng5rPa55w0rd
R1(config)# aaa new-model
R1(config)# aaa authentication login default group tacacs+
R1(config)# aaa authorization exec default group tacacs+
R1(config)# aaa authorization network default group tacacs+
R1(config)# aaa accounting exec default start-stop group tacacs+
R1(config)# aaa accounting network default start-stop group tacacs+
```

Рисунок 7.11 – Серверний облік

Доступ до LAN може бути захищений з використанням протоколу IEEE 802.1X. **Протокол 802.1X** – це протокол автентифікації і контролю доступу на основі портів, який обмежує для неавторизованих робочих станцій можливість підключатися до локальної мережі через загальнодоступні порти комутатора.

```
Router(config)# aaa accounting {network | exec | connection} {default | list-name} {start-stop
| stop-only | none } [broadcast] method1...[method4]
```

```
R1(config)# aaa accounting exec ?
  WORD Named Accounting list.
  default The default accounting list
```

```
R1(config)# aaa accounting exec default start-stop ?
  broadcast Use Broadcast for Accounting
  group     Use Server-group

R1(config)# aaa accounting exec default start-stop group ?
  WORD    Server-group name
  radius  Use list of all Radius hosts.
  tacacs+ Use list of all Tacacs+ hosts.
```

Рисунок 7.12 – Варіанти команд серверного обліку

7.1.4. Забезпечення безпеки з використанням автентифікації 802.1X

Стандарт IEEE 802.1X визначає контроль доступу на основі портів і протокол автентифікації, який забороняє робочим станціям, які не пройшли авторизацію, підключатися до LAN через загальнодоступні порти комутатора. Сервер автентифікації проводить автентифікацію кожної робочої

станції, яка підключається до порту комутатора, перш ніж надавати будь-які сервіси комутатора або LAN.

На рисунку 7.13 показано, що в процедурі автентифікації на базі портів 802.1X пристрою в мережі мають певні ролі:

– **Запитуючий пристрій (клієнт).** Пристрій (робоча станція), яка запитує доступ до сервісів LAN і комутатора і відповідає на запити комутатора. На робочій станції повинно використовуватися клієнтське ПЗ, сумісне зі стандартом 802.1X. (Порт, до якого підключається клієнт, є запитуючою пристроєм [клієнтом] згідно специфікації IEEE 802.1X.)

– **Автентифікатор (комутатор).** Контролює фізичний доступ до мережі, керуючись станом автентифікації вузла мережі. Комутатор виступає в ролі посередника (проксі-сервера) між клієнтом (запитуючою пристроєм) і сервером автентифікації. Він запитує у клієнта ідентифікаційні дані, перевіряє їх на сервері і ретранслює клієнту відгук сервера. У складі комутатора є програмний агент RADIUS, який відповідає за інкапсуляцію і декапсуляцію кадрів EAP (розширюваний протокол автентифікації), а також за взаємодію з сервером автентифікації.

– **Сервер автентифікації.** Безпосередньо виконує автентифікацію клієнта. Сервер автентифікації перевіряє справжність клієнта і повідомляє комутатора, чи є у клієнта повноваження на доступ до сервісів LAN і комутатора. Оскільки комутатор виступає в якості проксі-сервера, служба автентифікації для клієнта прозора. Система безпеки RADIUS з розширеннями EAP – єдиний підтримуваний сервер автентифікації.

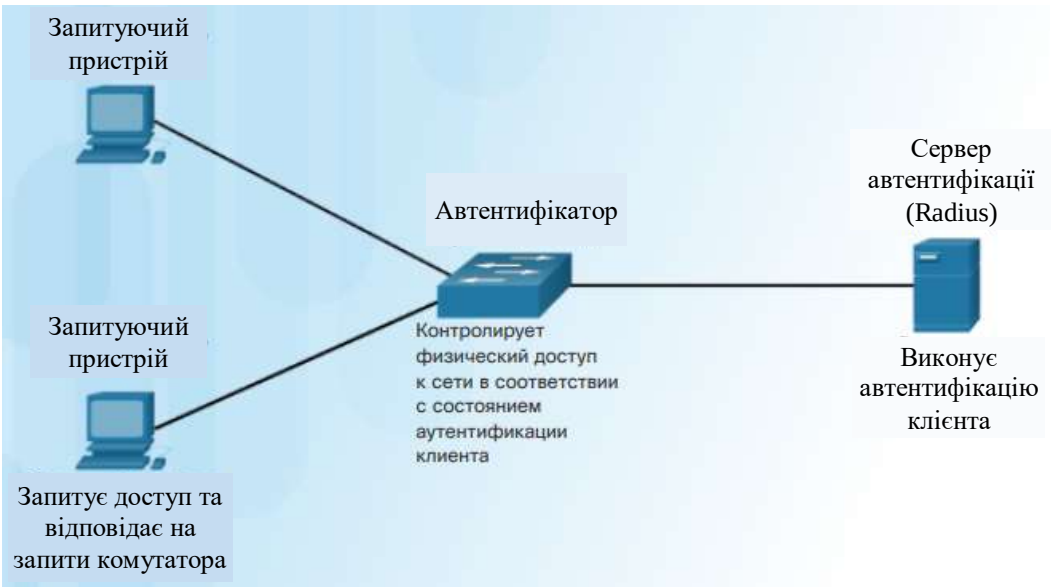


Рисунок 7.13 – Автентифікація пристрою в мережі на базі портів 802.1X

До проходження автентифікації робочої станції засоби контролю доступу 802.1X пропускають через порт тільки трафік протоколу розширеної автентифікації у LAN (EAPOL). Після успішної автентифікації дозволяється пересилання через порт звичайного трафіку.

Стан порту комутатора визначає, чи надана клієнту доступ в мережу. Під час налаштування для автентифікації 802.1X на базі портів початковим станом порту є неавторизований стан. У цьому стані порт забороняє весь вхідний і вихідний трафік, крім пакетів протоколу 802.1X. Після успішної автентифікації клієнта порт переходить в авторизований стан, і весь трафік клієнта може пересилатися звичайним чином. Якщо комутатор запитує ідентифікацію клієнта (ініціюється аутентифікатором) і клієнт не підтримує 802.1X, порт залишається в неавторизованому стані, і клієнтові не надається доступ до мережі.

Якщо ж клієнт з підтримкою 802.1X підключається до порту і ініціює процес автентифікації (запит ініціюється пристроєм), відправляючи кадр початкового стану EAPOL на комутатор з протоколом 802.1X і ніякої відповіді не надсилається, то клієнт починає відправляти кадри, як якщо б порт знаходився в авторизованому стані.

На рисунку 7.14 показаний повний процес обміну повідомленнями між запитуючим пристроєм, автентифікатором і сервером автентифікації. Інкапсуляція відбувається наступним чином:

– *Між запитуючим пристроєм і автентифікатором* – дані EAP інкапсулюються в кадри EAPOL.

– *Між аутентифікатором і сервером аутентифікації* – дані EAP інкапсулюються з використанням RADIUS.

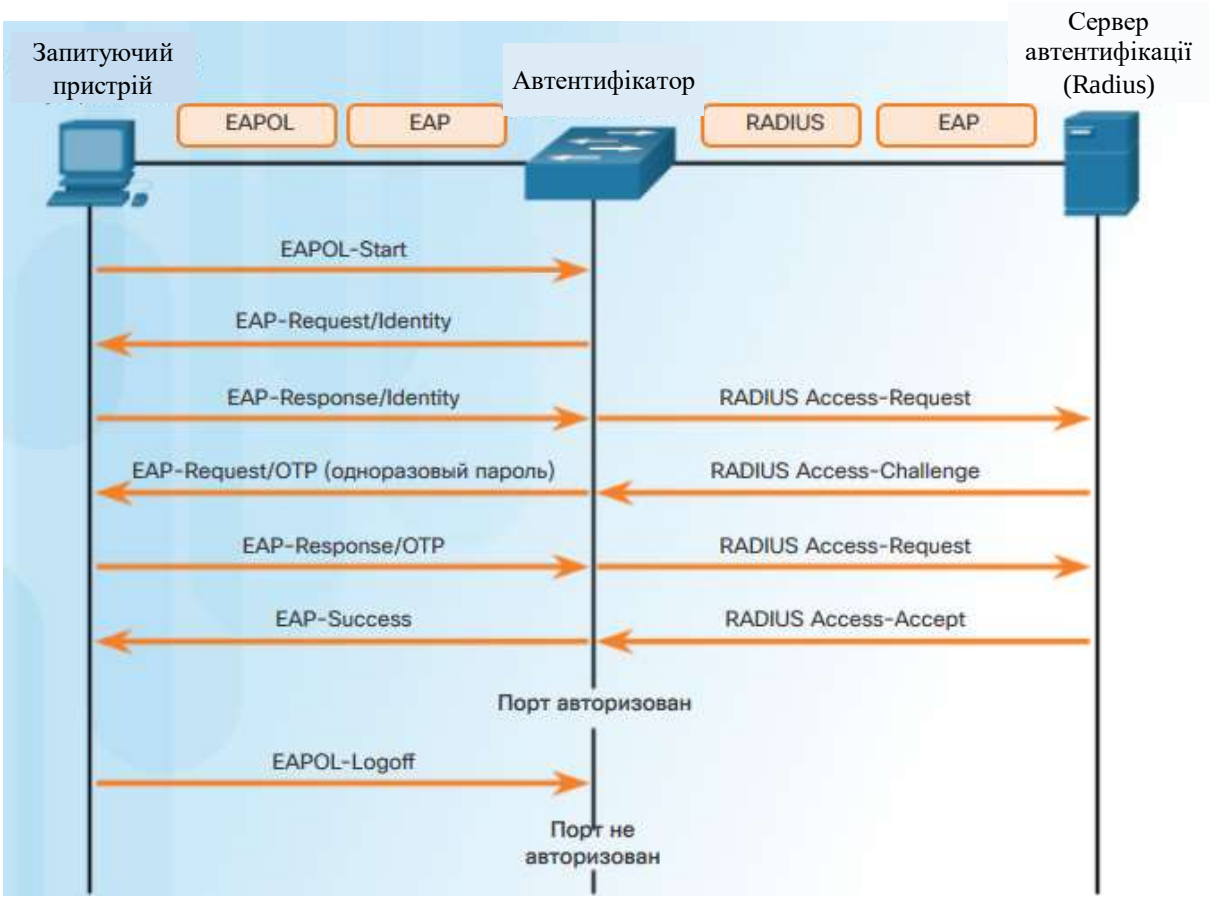


Рисунок 7.14 – Повний процес обміну повідомленнями між запитуючим пристроєм, автентифікатором і сервером автентифікації

Стани авторизації портів 802.1X

Команда **authentication port-control** дозволяє управляти порядком авторизації порту. На рисунку 7.15 показані синтаксис команди і опис параметрів. За замовчуванням порт знаходиться в стані **примусової авторизації** (**force-authorized**), тобто може відправляти і приймати трафік без автентифікації 802.1x.

```
S1(config-if)# authentication port-control ?
  auto                 PortState set to automatic
  force-authorized     PortState set to AUTHORIZED <--default
  force-unauthorized   PortState set to UnAuthorized

S1(config-if)# authentication port-control
```

Рисунок 7.15 – Синтаксис команди **authentication port-control**

Ключове слово **auto** необхідно ввести для включення автентифікації 802.1X. При успішному проходженні автентифікації клієнтом (отриманні кадру прийняття від сервера автентифікації) стан порту змінюється на авторизований, і всі кадри від клієнта, який пройшов автентифікацію, оброблюються на порту.

При відмові в автентифікації порт залишається в неавторизованому стані, але автентифікація може бути проведена повторно. У тих випадках, коли сервер автентифікації недоступний, комутатор може повторити відправку запиту. Якщо до сервера не вдалося звернутися після певного числа повторів, автентифікація вважається не пройденою, і доступ до мережі не надається.

Після завершення роботи клієнта він відправляє повідомлення виходу EAPOL, в результаті чого порт комутатора повертається в неавторизований стан.

Якщо стан порту змінюється на **відключений** (**force-unauthorized**) або порт отримує кадр виходу EAPOL, то порт повертається в неавторизований стан.

Налаштування авторизації портів 802.1X

Для налаштування авторизації портів 802.1X необхідно виконати наступну процедуру (рисунок 7.16):

Крок 1. Увімкнути AAA за допомогою команди **aaa new-model**.

Крок 2. Призначити сервер RADIUS та налаштувати його адресу та порти.

Крок 3. Створити список методів автентифікації на основі портів 802.1X за допомогою команди **aaa authentication dot1x**.

Крок 4. Увімкнути глобальну автентифікацію на основі портів 802.1X за допомогою команди **dot1x system-auth-control**.

Крок 5. Дозволити автентифікацію на основі порту в інтерфейсі за допомогою команди **authentication port-control auto**.

Крок 6. Увімкнути автентифікацію 802.1X на інтерфейсі за допомогою команди **dot1x pae**. Параметри автентифікатора встановлюють тип сутності доступу до порту (PAE), тому інтерфейс діє лише як автентифікатор і не реагує на повідомлення, призначені для запитуючого пристрою.

```
S1(config)# aaa new-model
S1(config)# radius server NETSEC
S1(config-radius-server)# address ipv4 10.1.1.50 auth-port 1812 acct-port 1813
S1(config-radius-server)# key RADIUS-Pa55w0rd
S1(config-radius-server)# exit
S1(config)#
S1(config)# aaa authentication dot1x default group radius
S1(config)# dot1x system-auth-control
S1(config)#
S1(config)# interface F0/1
S1(config-if)# description Access Port
S1(config-if)# switchport mode access
S1(config-if)# authentication port-control auto
S1(config-if)# dot1x pae authenticator
```

Рисунок 7.16 – Приклад налаштування авторизації портів 802.1X

Контрольні питання до розділу 7

1. Опишіть та проаналізуйте методи аутентифікації без застосування процедур AAA.
2. Охарактеризуйте призначення, застосування та основні відмінності протоколу RADIUS.
3. Опишіть та проаналізуйте реалізацію безпеки ресурсів мережі за стандартом 802.1X.
4. Наведіть команди та опишіть їх призначення при реалізації серверної аутентифікації через TACACS+.
5. Наведіть команди та опишіть особливості реалізації серверної аутентифікації за списком за замовченням та за іменованним списком.

СПИСОК ВИКОРИСТАНОЇ ДЖЕРЕЛ

1. Романов А.И. Телекомунікаційні мережі та управління : навчальний посібник. Київ : ВПЦ “Київський університет”, 2003. 247 с.
2. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі : навчальний посібник. Київ : “Техніка”, 2001. 526 с.
3. Стеклов В.К., Беркман Л.Н. Проектування телекомунікаційних мереж: навчальний посібник. Київ : “Техніка”, 2003. 923 с.
4. Наталенко П.П. Телекомунікаційні та інформаційні мережі : навчальний посібник. Київ : ВІТІ, 2011. 384 с.
5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. СПб : Питер, 2010. 984 с.
6. Программа сетевой академии CISCO CCNA 1 и 2. М. : Вильямс, 2006. 1168 с.
7. Программа сетевой академии CISCO CCNA 3 и 4. М. : Вильямс, 2008. 876 с.
8. Воробієнко П.П., Нікітюк Л.А., Резніченко П.І. Телекомунікаційні та інформаційні мережі: Підручник [для вищих навчальних закладів] Київ : САММІТ-Книга, 2010. 708 с.
9. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М. : Радио и связь, 2000. 500 с.
10. Назаров А.Н., Симонов М.В. АТМ технология высоких скоростей. М. : ЭКО-ТРЕНДЗ, 1998. 254 с.
11. Будылдина Н.В., Шувалов В.П. Телекоммуникационные сети с многопротокольной коммутацией по меткам. Построение и оптимизация. Екатеринбург : УрТИСИ ГОУ ВПО “СибГУТИ”, 2006. 274 с.
12. Бакланов И.Г. NGN: принципы построения и организации / под ред. Ю.Н. Чернышова. М. : Эко-Трендз, 2008. 400 с. : ил.
13. Голь В.Д., Толстова А.В. Телекомунікаційні та інформаційні мережі. Керівництво з лабораторних занять та курсового проектування. Київ : ІСЗЗІ КПІ ім. Ігоря Сікорського, 2019. 45 с.
14. Уэнстром М. Организация защиты сетей Cisco : Пер. с англ. М. : Издательский дом “Вильямс”, 2005. 768 с. :ил., С. 257…261.
15. Росляков А.В. и др. Сети следующего поколения NGN / под ред. А.В. Рослякова. М. : Эко-Трендз, 2009, 424 с. : ил.
16. Макаренко С.И., Федосеев В.Е. Системы многоканальной связи. Вторичные сети и сети абонентского доступа : учебное пособие СПб. : ВКА имени А.Ф. Можайского, 2014. 179 с.
17. Технологічна документація LLD IP-MPLS.
18. Інформаційна база спеціальної кафедри № 3 (локальний доступ).

ПРИМІТКИ