Державний університет Телекомунікацій
Навчально-науковий інститут телекомунікацій

Навчальний посібник

для самостійної роботи з дисципліни

“ТЕЛЕКОМУНІКАЦІЙНІ СИСТЕМИ ТА МЕРЕЖІ НАСТУПНОГО ПОКОЛІННЯ”

Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О.

Київ – 2019

УДК 621.391.13
В 685
ББК 32.811

Гриф надано
Державним університетом телекомунікацій
(*протокол № від 2013 р.*)

Рецензенти: проф., д.т.н.
проф., д.т.н.

Навчальний посібник призначений для самостійної роботи студентів вищих навчальних закладів за кредитно-модульною організацією навчального процесу з навчальної дисципліни “Телекомунікаційні системи та мережі наступного покоління” (ТСМНП) - циклу дисциплін професійної та практичної підготовки за напрямом 0924 “ТЕЛЕКОМУНІКАЦІЇ”.

Заїка В.Ф., Варфоломеєва О.Г., Домрачева К.О., Гринкевич Г.О.

У посібнику досліджено загальні характеристики інфокомунікаційних мереж та полуг, розглянуто основні завдання та функції мережі настурного покоління, її архітектуру, проаналізовано особливості реалізації сучасних телекомунікаційних технологій на рівнях транспорту, управління та доступу. Наведено основні моделі забезпечення якості надання послуг, в тому числі архітектуру інтегрованого та диференційного обслуговування.

Контрольні питання і задачі допоможуть студенту в підготовці до модульного контролю.

Навчальний посібник призначений для студентів, які навчаються за спеціальностями з напряму “Телекомунікації”, а також може бути корисний для аспірантів, викладачів навчальних закладів відповідних спеціальностей, фахівців, які обслуговуть телекомунікаційні мережі зв'язку.

ЗМІСТ

ВСТУП

Глобалізація та інші сучасні тенденції розвитку телекомунікаційних мереж призвели не лише до значного переносу основних телекомунікаційних концепцій, але й до значних технологічних зсувів, а саме: від мовного трафіку до трафіку даних та мультимедійного трафіку, від спеціалізованих до глобальних інфокомунікаційних мереж, від локальних спеціалізованих послуг до мультимедійних універсальних послуг та додатків з гарантованою якістю в будь-який час в будь-якому місці.

Введена міжнародним союзом електрозв'язку ITU-T (International Telecommunication Union – Telecommunication standardization sector) концепція мережі наступного покоління NGN (Next Generation Network), визначає архітектуру апаратних і програмних засобів, що передбачає обмін викликами спеціальних процедур між комутаційною системою і мережею під час організації зв'язку. Виконання цих процедур може управляти процесами комутації і іншими мережевими ресурсами з метою виконання функцій «інтелектуальної» маршрутизації, тарифікації, взаємодії з користувачем

Мережа наступного покоління забезпечує передавання всіх видів медіатрафіку та розподілене надання необмеженого спектру інфокомунікаційних послуг з можливістю їх масштабування, управління та розподіленої тарифікації. Мережа підтримує передавання трафіку з різними вимогами до якості обслуговування та підтримує вибрані користувачем вимоги до надаваних послуг. Поява програмних комутаторів повністю змінила архітектуру, склад обладнання та методи побудови телекомунікаційних мереж. Передавання мовного, аудіосигналу, сигналу зображень мережами з комутацією пакетів поставило перед виробниками апаратно-програмних комплексів, специфічні завдання, які можуть вирішуватись за рахунок вдосконалення алгоритмів та програмного забезпечення. Це перш за все оброблення сигналів у реальному часі або з постійною затримкою. Можливості сучасних процесорів цифрової обробки сигналів дозволяють з високою ефективністю реалізувати оптимальні алгоритми стиснення/відновлення сигналів, сигналізацію, сучасні протоколи.

Відмінна особливість ідеології NGN – використання технології IP (Internet Protocol) для передачі та для комутації. Ця властивість NGN стимулює розробку принципів побудови інфокомунікаційних мереж, які відповідають таким вимогам:

– можливість поетапного перетворення транспортних і телефонних мереж, які є в даний час основою системи телекомунікацій в Україні;

– збереження інвестицій операторів телекомунікацій, які були направлені на розвиток транспортних і телефонних мереж в попередні роки;

– здатність надати потенційним клієнтам сучасні види інфокомунікаційних послуг для забезпечення високої конкурентоспроможності експлуатаційних компаній;

– мінімізація витрат на побудову мереж NGN та їх поетапний розвиток.

Книга побудована таким чином, що в ній можна умовно виділити декілька частин. В перших двох розділах проведений аналіз необхідності переходу до інфокомунікаційних мереж і послуг, розглянуті основні вимоги до мереж наступного покоління, приведена ієрархічна модель побудови NGN.

Подальші розділи розглядають технології, за допомогою яких NGN може бути реалізована на транспортному рівні (розділ 4), на рівні доступу (розділ 5) і на рівні управління (розділ 7). У розділі 2 розглядаються особливості стека протоколів TCP/IP (в основному транспортний і мережевий рівні стека), і, нарешті, в розділі 6 наводяться основні принципи і моделі забезпечення якості послуг (QoS).

Розділ 1. Загальні принципи організації мережі наступного покоління

1.1. Передумови переходу до мереж NGN

Результатом еволюції телекомунікаційної індустрії з'явився перехід від телекомунікаційної мережі до Глобальної інформаційної інфраструктури, від телекомунікаційних послуг до інфокомунікаційных послуг. Технологічною основою інформаційного суспільства є Глобальна Інформаційна Інфраструктура (Global Information Infrastructure, GII), яка повинна забезпечити можливість бездискримінаційного доступу до інформаційних ресурсів кожному жителю планети. Інформаційну інфраструктуру складає сукупність баз даних, засобів обробки інформації, взаємодіючих мереж зв'язку і терміналів користувачів. Доступ до інформаційних ресурсів в GII реалізується за допомогою послуг зв'язку нового типа, що отримали назву послуг Інформаційного суспільства або інфокомунікаційних послуг.

Користувачі дістали доступ до послуг, про які 10–15 років тому і не замислювалися. E-mail, Інтернет, стільниковий телефон сталі звичайними атрибутами повсякденного життя. Нам вже недостатньо просто поговорити по домашньому телефону. Ми хочемо мати можливість подзвонити своїм друзям або колегам, знаходячись в будь-якій точці земної кулі. Вже недостатньо мати декілька різних номерів, що належать різним мережам. Бажано мати один персональний номер, який дозволяв би однозначно визначати нас і направляти вхідний дзвінок до терміналу, підключеного до мережі, в якій ми знаходимося в даний момент.

Але якими б не були наші бажання, а також досягнення в науці і техніці, жоден оператор зв'язку не встановлюватиме нове устаткування або не вводитиме нові сервіси, якщо це економічно недоцільно. Тому потреба операторів мереж зв'язку отримувати все нові прибутки заставляє їх задуматися над створенням мережі, яка дозволяла б:

- щонайшвидше і дешевше створювати нові послуги з тим, аби постійно залучати нових абонентів;
- зменшувати витрати на обслуговування;
- бути незалежними від постачальників устаткування;
- бути конкурентоздатними (дерегуляція в телекомунікаційній галузі і досягнення в новітніх технологіях привели до появи нових операторів зв'язку і сервіс-провайдерів, що пропонують дешевший і ширший спектр послуг).

Інфокомунікаційна послуга – послуга зв'язку, що передбачає автоматизовану обробку, зберігання або надання по запиту інформації з використанням засобів обчислювальної техніки, як на вхідному, так і на вихідному кінці з'єднання (Directive 98/48/EC of the European Parliament of 20 July 1998).

На сьогоднішній день розвиток інфокомунікаційних послуг здійснюється, в основному, в рамках комп'ютерної мережі Інтернет, доступ до послуг якої відбувається через традиційні мережі зв'язку. В той же час у ряді випадків послуги Інтернет, зважаючи на обмежені можливості її транспортної інфраструктури, не відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства. У зв'язку з цим розвиток інфокомунікаційних послуг вимагає вирішення завдань ефективного управління інформаційними ресурсами з одночасним розширенням функціональності мереж зв'язку. У свою чергу це стимулює процес інтеграції Інтернету і мереж телекомунікацій.

До основних технологічних особливостей, що відрізняють інфокомунікаційні послуги від послуг традиційних мереж зв'язку, можна віднести наступні:

- інфокомунікаційні послуги виявляються на верхніх рівнях моделі ВВС – Взаємодії Відкритих Систем (тоді як послуги зв'язку надаються на третьому, мережному рівні);
- більшість інфокомунікаційних послуг передбачають наявність клієнтської і серверної частин; клієнтська частина реалізується в устаткуванні користувача, а серверна – на спеціальному виділеному вузлі мережі, званому вузлом служб;
- інфокомунікаційні послуги, як правило, передбачають передачу інформації мультимедіа, яка характеризується високими швидкостями передачі і несиметричністю вхідного і вихідного інформаційних потоків;
- для надання інфокомунікаційних послуг частенько необхідні складні багатоточечні конфігурації з'єднань;
- для інфокомунікаційних послуг характерна різноманітність прикладних протоколів і можливостей щодо управління послугами з боку користувача;
- для ідентифікації абонентів інфокомунікаційних послуг може використовуватися додаткова адресація в рамках даної інфокомунікаційної послуги.

Більшість інфокомунікаційних послуг є "додатками", тобто їх функціональність розподілена між устаткуванням постачальника послуги і

граничним устаткуванням користувача. Як наслідок, функції граничного устаткування також мають бути віднесені до складу інфокомунікаційної послуги, що необхідно враховувати при їх регламентації.

Бізнес-модель, що визначає учасників процесу надання інфокомунікаційних послуг і їх взаємовідношення, також відрізняється від моделі традиційних послуг електрозв'язку, в якому було представлено всього лише три основні учасники: оператор, абонент і користувач. Нова бізнес-модель передбачає наявність постачальника послуг, який надає інфокомунікаційні послуги абонентам і користувачам. При цьому сам постачальник є споживачем послуг перенесення, що надаються оператором телекомунікаційної мережі.

На ринку можуть бути також присутніми додаткові види постачальників послуг: постачальники інформації, брокери, рітейлери і так далі Постачальник інформації надає інформацію постачальникові послуг для поширення. Брокер надає інформацію про постачальників послуг і їх потенційних абонентів, сприяє користувачам в пошуку постачальників, що надають необхідні послуги. Рітейлер виступає як посередник між абонентом і постачальником з метою адаптації послуги до індивідуальних вимог абонента.

До інфокомунікаційних послуг пред'являються такі вимоги, як:

- мобільність послуг;
- можливість гнучкого і швидкого створення нових послуг;
- гарантована якість послуг.

Великий вплив на вимоги до інфокомунікаційних послуг має процес конвергенції, що призводить до того, що інфокомунікаційні послуги стають доступними користувачам незалежно від способів доступу.

Зважаючи на розглянуті особливості інфокомунікаційних послуг, можуть бути визначені наступні вимоги до перспективних мереж зв'язку:

- мультисервисність, під якою розуміється незалежність технологій надання послуг від транспортних технологій;
- широкосмуговість, під якою розуміється можливість гнучкої і динамічної зміни швидкості передачі інформації в широкому діапазоні залежно від поточних потреб користувача;
- мультимедійність, під якою розуміється здатність мережі передавати багатокомпонентну інформацію (мова, дані, відео, аудіо) з необхідною синхронізацією цих компонент в реальному часі і використанням складних конфігурацій з'єднань;
- інтелектуальність, під якою розуміється можливість управління послугою, викликом і з'єднанням з боку користувача або постачальника послуг;

- інваріантність доступу, під якою розуміється можливість організації доступу до послуг незалежно від використовуваної технології;
- багатооператорність, під якою розуміється можливість участі декількох операторів в процесі надання послуги і розділення їх відповідальності відповідно до області діяльності.

Крім того, при формуванні вимог до перспективних мереж зв'язку необхідно враховувати особливості діяльності постачальників послуг. Зокрема, сучасні підходи до регламентації послуг приєднання передбачають доступ постачальників послуг, у тому числі і тих, що не володіють власною інфраструктурою, до ресурсів мережі загального користування на недискримінаційній основі. При цьому до основних вимог, що пред'являються постачальниками послуг до мережного оточення, відносяться:

- забезпечення можливості роботи устаткування в "мультиоператорському" середовищі, тобто збільшення числа інтерфейсів для підключення до мереж відразу декількох операторів зв'язку, у тому числі на рівні доступу;
- забезпечення взаємодії вузлів постачальників послуг для їх спільного надання;
- можливість вживання "масштабованих" технічних рішень при мінімальній стартовій вартості устаткування.

Існуючі мережі зв'язку загального користування з комутацією каналів (ТФЗК) і комутацією пакетів (СПД) в даний час не відповідають перерахованим вище вимогам. Обмежені можливості традиційних мереж є стримуючим чинником на шляху впровадження нових інфокомунікаційних послуг.

З іншого боку, нарощування обсягів інфокомунікаційних послуг, що надаються, може негативно позначитися на показниках якості обслуговування викликів базових послуг існуючих мереж зв'язку.

Все це вимушує враховувати наявність інфокомунікаційних послуг при плануванні способів розвитку традиційних мереж зв'язку у напрямі створення мереж зв'язку наступного покоління.

Розвиток інфокомунікаційних послуг вимагає вирішення завдань ефективного управління інформаційними ресурсами з одночасним розширенням функціональності телекомунікаційних мереж. У 90-х роках минулого століття передбачалося, що ідея створення інфокомунікаційних мережі буде втілена за допомогою концепції інтелектуальної мережі. У 1993 році Міжнародний союз електрозв'язку (ITU-T) затвердив перші специфікації технології Intelligent Network (IN). Основним принципом побудови інтелектуальної мережі стало логічне розділення рівня комутації і надання послуг, завдяки чому з'явилася

можливість створювати нові телекомунікаційні послуги відповідно до специфічних для кожної з них вимогами до мережі і абонентських пристроїв.

Фізична архітектура IN передбачає наявність наступних компонентів (рис.1.1):

- SSP (Service Switching Point) - вузол комутації послуг, що може бути представлений як АТС з відповідною версією програмного забезпечення, яка виконує функцію управління викликом і функцію комутації послуги; тобто SSP є звичайною комутаційною станцією, в якій зберігаються всі функції управління процесом надання основних послуг зв'язку, оснащену додатковими програмними засобами. SSP забезпечує доступ абонентів мережі зв'язку до послуг IN і підтримує протоколи взаємодії з іншими елементами IN. SSP визначає, що прийнятий їм від абонента виклик вимагає звернення до послуг IN, і направляє відповідний запит у вузол управління послугами SCP. Запит може містити номер викликаючого абонента, набрані ним цифри номера, код необхідної послуги і інші параметри. Після оснащення комутаційного устаткування функціями SSP послуги IN можуть вводитися і віддалятися шляхом відповідних змін конфігурації SSP, які здійснюються технічним персоналом через звичайний інтерфейс оператора.
- SCP (Service Control Point) - вузол управління послугами (контролер послуг), обробляє дані і формує відповідні команди; SCP містить програмні засоби, які централізовано реалізують логіку послуг і підтримують протоколи взаємодії з іншими елементами мережі. SCP приймає запит від SSP і повертає йому інструкції для подальшої обробки виклику відповідно до логіки затребованої послуги. До прийому від SCP потрібних інструкцій обслуговування виклику в SSP припиняється. SCP відповідає за обслуговування виклику до тих пір, поки управління з'єднанням не буде передано назад в SSP.
- SDP (Service Data Point) - вузол бази даних послуг, що містить дані, які використовуються програмами логікі послуги, аби забезпечити індивідуальність послуги;
- IP (Intelligent Peripheral) - інтелектуальна периферія IP виконує допоміжні функції, що підтримують діалог з абонентом, такі як передача запрошення до набору додаткових цифр, прийом цифр, що передавалися абонентом багаточастотним способом (DTMF), розпізнавання мови і деякі інші. Інтелектуальна периферія може бути вбудована в SSP, або реалізована у відособленому устаткуванні. IP управляється з боку SCP за протоколом INAP. Для підключення IP до SSP використовуються з'єднувальні лінії з сигналізацією,

підтримуваною підсистемою ISUP системи ОКС–7, або лінії первинного доступу ISDN з цифровою абонентською сигналізацією DSS1 (30B+D=30×64+16=2 Мбіт/с).

- SMP (Service Management Point) - вузол експлуатаційного управління послуг, що надає операторові мережі можливості контролю і управління параметрами та конфігурацією послуг IN. SMP забезпечує експлуатаційне управління діючими послугами, а також плануванням нових послуг і їх введенням.
- SCEP (Service Creation Environment Point) - вузол середовища створення послуг, який виконує функцію середовища створення послуг і служить для розробки, формування і впровадження послуг в пункті їх забезпечення SMP. Середовище створення послуг містить засоби конструювання, модифікації і тестування послуг до початку комерційної експлуатації, а також засоби завантаження відповідних програм в SMP. Протоколи взаємодії між SMP, SCEP і SCP Міжнародним союзом електрозв'язку доки не визначені, проте стандартними протоколами де факто став протокол TCP/IP.

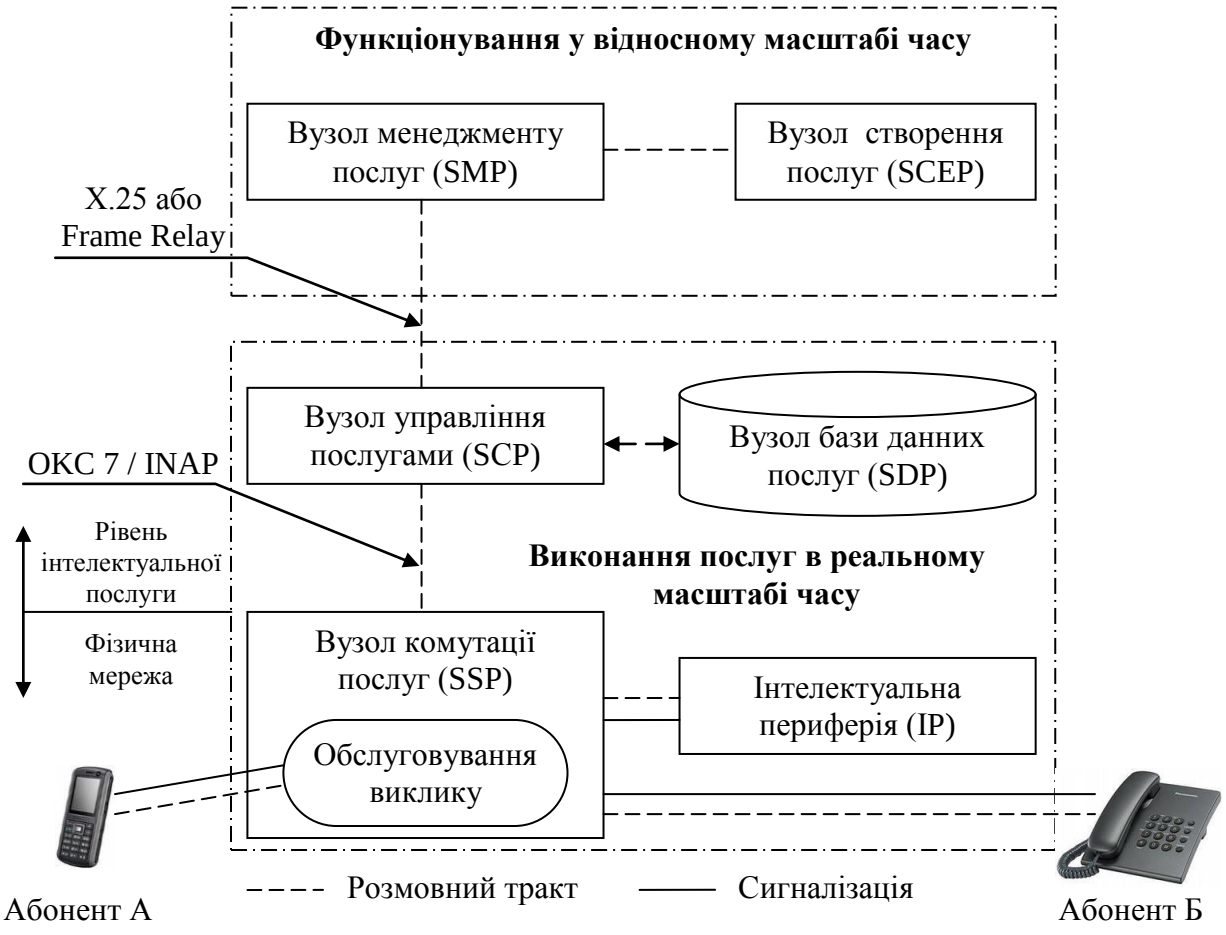


Рис.1.1. Платформа Інтелектуальної мережі

Схематично виклик здійснюється таким чином. Абонент знімає трубку і набирає номер. SSP приймає виклик і починає його обробку. Наштовхнувшись на запит, SSP припиняє виконання виклику і звертається до SCP за інструкціями. Після отримання необхідної інформації, наприклад про маршрутизацію виклику, SSP продовжує його виконання до завершення виклику.

Процедура здійснення виклику, тобто встановлення, підтримки і розриву з'єднання, складається з декількох етапів або станів: "вільно", "зняття трубки", "набір номеру", "аналіз номеру", "маршрутизація виклику" і так далі. Запит на послугу може бути вставлений в так звані моменти ініціації запиту. Принципово ця модель здійснення виклику нічим не відрізняється від тієї, що використовувалася до появи концепції інтелектуальної мережі. Головна її відмінність в стандартизації.

Процедуру виклику ми розглянемо на прикладі служби "Не турбувати" (рис. 1.2). На прохання абонента SCP проводить вибіркове блокування викликів, що поступають. Отримавши виклик для абонента, телефонний комутатор на завершуючому кінці з'єднання звертається до SCP із запитом про те, що йому робити з цим викликом. SCP визначає, що наведений номер телефону відсутній в списку дозволених номерів, тому він передає SSP інструкцію відтворити записане повідомлення. В результаті викликаюча сторона чує повідомлення: "Абонент тимчасово недоступний. Перетелефонуйте, будь ласка, пізніше".

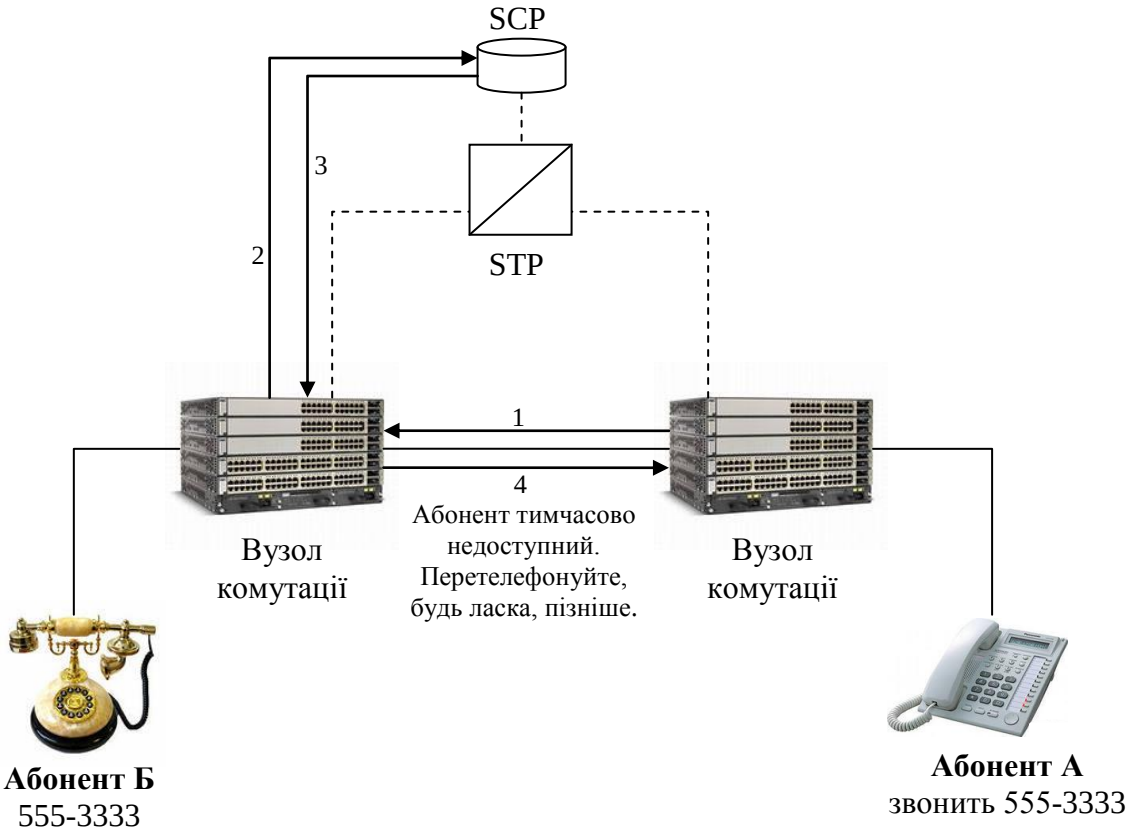


Рис. 1.2. Приклад реалізації сервісу "Не турбувати".

Концепція IN дозволила телефонним операторам значно розширити спектр послуг, але мала ряд недоліків:

- Номенклатура послуг виявилася повністю залежною від можливостей прикладного протоколу INAP (Intelligent Network Application Protocol), за допомогою якого реалізуються функції інтелектуальних платформ. В разі доопрацювання INAP при додаванні нової послуги оператором була потрібна модернізація всіх мережних вузлів комутації і управління послугами (SSP і SCP).
- Складністю процесу створення послуг. Відсутність стандартизованого інтерфейсу між SCEP і SCP зробила практично неможливою або важко здійснюваною розробку нових послуг і модифікації тих, що існують.
- Неповне дотриманням стандартів IN виробниками устаткування, зокрема, низька сумісність рішень щодо розробки вузлів SSP і SCP різних виробників.
- Послуги можна замовити лише за допомогою спілкування з інтелектуальною периферією (комп'ютером).
- Програмно-апаратна платформа IN знаходиться у веденні базового оператора зв'язку, і її ресурси не завжди можуть виділятися третій стороні – постачальникам послуг.
- Необхідність істотних початкових інвестицій для створення Інтелектуальної мережі і загальною високою вартістю її інфраструктури.
- Конкуренція з боку NGN. Вигідніше розміщувати бази даних і логіку послуг в IP - області.

З розвитком інфокомунікаційних послуг ідея об'єднання телефонних мереж, мобільному зв'язку, Internet, отримала свій розвиток в концепції NGN (Next Generation Network), в основу якої був покладений принцип відділення функцій перенесення і комутації, функцій управління викликом і функцій управління послугами.

1.2. Поняття мережі NGN, характеристики NGN

В основу концепції побудови мережі зв'язку наступного покоління покладена ідея про створення універсальної мережі, яка б дозволяла переносити будь-які види інформації, такі як мова, відео, аудіо, графіку і т. д., а також забезпечувати можливість надання необмеженого спектру інфокомунікаційних послуг.

Мережа зв'язку наступного покоління NGN – Next Generation Network – мережа з пакетною комутацією, придатна для надання послуг електрозв'язку і

для використання декількох широкосмугових технологій транспортування з включеною функцією QoS, в якій функції, що пов'язані з обслуговуванням, не залежать від технологій, що застосовуються для забезпечення транспорту. Вона забезпечує вільний доступ користувачів до мереж і конкуруючих постачальників послуг. Вона підтримує універсальну мобільність, яка забезпечує постійне і повсюдне надання послуг користувачам. (ITU-T Rec. Y.2001)

Базовим принципом концепції NGN є відділення один від одного функцій перенесення і комутації, функцій управління викликом і функцій управління послугами.

NGN, яка потенційно повинна об'єднати існуючі мережі зв'язку (телефонні мережі загального користування – ТФОП, мережі передачі даних – СПД, мережі рухливого зв'язку – СПС), має наступні характеристики:

- Мережа на базі комутації пакетів, яка має розділені функції управління і перенесення інформації, де функції послуг і застосувань відокремлені від мережних функцій.
- Мережа, в якій усі компоненти зв'язані за допомогою відкритих інтерфейсів.
- Мережа, що підтримує широкий спектр послуг, включаючи послуги в реальному часі і послуги доставки інформації (e-mail), у тому числі мультимедіа послуги.
- В цій мережі реалізована конвергенція фіксованого і рухливого зв'язку.
- Мережа що має властивість загальної мобільності.
- Мережа, що дозволяє окремому абонентові користуватися і управляти послугами незалежно від технології доступу і типа використовуваного терміналу.
- В NGN функції постачальника послуг відокремлено від функцій оператора мережі. При цьому під оператором будемо розуміти підприємство, що надає користувачеві фізичний ресурс мережі і забезпечує доступ абонентів до послуг постачальників послуг, а під постачальником послуг – підприємство, що розробляє і просуває послугу.
- Мережа, що надає абонентові можливість вільного вибору постачальника послуг.

Мережі, побудовані на основі концепції NGN, мають наступні переваги перед традиційними мережами електрозв'язку.

- NGN дозволяє побудову і використання однієї універсальної мережі для надання різних послуг;
- Оператор NGN може найбільш оптимально реалізовувати смугу пропускання для інтеграції різних видів трафіку і надання різних послуг;
- NGN краще пристосована до модернізації і розширення;

- Оператор NGN має в своєму розпорядженні можливість швидкого впровадження нових послуг.
- Для користувача не має значення технологія, за якою реалізується послуга електрозв'язку (принцип чорного ящика).
- Забезпечується можливість гнучкого та швидкого створення нових послуг з необхідною якістю;
- Універсальна мобільність послуг NGN.

До спектру послуг NGN відносяться як існуючі послуги традиційного зв'язку, так і нові інформаційні послуги, включаючи:

- послуги служби телефонному зв'язку (надання місцевого телефонного з'єднання, міжміського телефонного з'єднання, міжнародного телефонного з'єднання);
- послуги служб передачі даних (надання виділеного каналу передачі даних, постійного і комутованого доступу в мережу Інтернет, віртуальних приватних мереж передачі даних);
- послуги телематичних служб ("електронна пошта ", "голосова пошта ", "доступ до інформаційних ресурсів ", телефонія по IP-протоколу, "аудіоконференція " і "відеоконференція ");
- послуги служб мобільного електрозв'язку;
- послуги постачальників інформації: відео і аудіо за запитом, "інтерактивні новини" (для користувача реалізується можливість перегляду, прослухування і читання інформації про події, що сталися за якийсь час), електронний супермаркет (користувач вибирає товар в "електронному магазині", отримує детальну інформацію про його споживчі властивості, ціні і ін.), дистанційне навчання та ін.

Таким чином, NGN підтримує як існуюче на даний час, так і нове кінцеве обладнання, включаючи аналогові телефонні апарати, факсимільні апарати, обладнання цифрової мережі з інтеграцією служб, стільникові телефони різних стандартів, термінали телефонії по IP-протоколу (SIP і H.323), кабельні модеми і так далі.

Розглянемо детальніше способи класифікації послуг мережі NGN.

1.3. Класифікація послуг для мереж NGN

В даний час відсутня загальна класифікація послуг для мереж NGN. В рамках концепції, коли мережу NGN пропонується розглядати не як окрему категорію мереж зв'язку, а як інструмент побудови і розвитку існуючих мереж,

послуги, що надаються в рамках фрагмента NGN, можна класифікувати таким чином:

- базові: послуги, орієнтовані на встановлення з'єднання з використанням фрагмента NGN між двома кінцевими терміналами;
- додаткові види обслуговування: послуги, що надаються разом з базовими і орієнтовані на підтримку додаткових списків можливостей (у зарубіжній літературі ДВО зазвичай іменується як VAS (Value Added Services) - послуги, що приносять додатковий прибуток.;
- послуги доступу, орієнтовані на організацію доступу до ресурсів, і точок присутності інтелектуальних мереж і мереж передачі даних, у тому числі:
  - інформаційно-довідкові послуги: послуги, орієнтовані на надання інформації з баз даних, що входять до структури NGN ;
  - послуги віртуальних приватних мереж: послуги, орієнтовані на організацію і підтримку функціонування VPN з боку елементів фрагмента NGN ;
  - мультимедійні послуги: послуги, орієнтовані на забезпечення і підтримку функціонування мультимедійних застосувань з боку фрагмента NGN.

Розглянемо базові послуги. Під базовими послугами розуміються:

- послуги місцевого, міжміського, міжнародного телефонного зв'язку, мережі, що надаються з використанням (повним або частковим) фрагмента, на основі NGN-технологій. Базові послуги телефонії можуть бути доступні користувачам, що використовують термінали мереж ТФЗК, СРЗ і H.323, SIP-термінали;
- послуги з передачі факсимільних повідомлень між термінальним обладнанням користувачів. Послуга може надаватися користувачам, що використовують термінали мереж ТФХК і СРЗ. Послуга віртуальний факс (e-fax, Fax-to-Email) не відноситься до даного класу;
- послуга доставки інформації "64 кбіт/с без обмежень" і послуги надання зв'язку, що базуються на ній, визначені для технології ISDN для встановлення з'єднань між термінальним устаткуванням користувачів. Послуга може надаватися користувачам, що використовують термінали ISDN.

Завданням мережного фрагмента NGN при наданні базових послуг є встановлення і підтримка з'єднання з необхідними параметрами.

Надання базових послуг може супроводжуватися додатковими видами обслуговування, які розширюють можливості користувача щодо здобуття

інформації про з'єднання, тональні повідомлення, а також дозволяють змінювати конфігурацію з'єднання. У мережному фрагменті NGN користувачам можуть бути доступні наступні додаткові види обслуговування:

- ідентифікація викликаючої лінії (CLIP – Calling Line Identity Presentation) - надання абонентові інформації про номер викликаючого абонента завжди, за винятком випадку, коли у викликаючого абонента встановлений ДВО на заборону ідентифікації викликаючої лінії;
- заборона ідентифікації викликаючої лінії (CLIR – Calling line identification restriction) надає викликаючому абонентові можливість тримати свій номер в секреті від абонента, що викликається, незалежно від наявності у абонента, що викликається, ДВО "ідентифікація номера викликаючого абонента";
- надання ідентифікації підключеної лінії (COLP – Connected Line identification Presentation). Викликаючий абонент не може бути упевнений в тому, що він сполучений саме з тим абонентом, номер якого він набирав, оскільки у абонента, що викликається, може бути активізований ДВО "перенаправлення виклику". ДВО "ідентифікація номера підключеної лінії" надає абонентові можливість для вихідного виклику отримувати інформацію про номер підключеної лінії. Інформація про номер підключеної лінії надається у момент відповіді абонента, що викликається, у вигляді повного номера абонента. Форма надання цього номера залежить від конкретного терміналу. Наявність у абонента даного ДВО гарантує надання йому інформації про номер підключеного терміналу завжди, за винятком випадку, коли у абонента, що викликається, встановлений ДВО "заборона ідентифікації підключеної лінії";
- заборона ідентифікації підключеної лінії (COLR – Connected Line identification restriction) надає абонентові, що викликається, можливість тримати свій номер в секреті від викликаючого абонента незалежно від наявності у нього ДВО "ідентифікація номера підключеної лінії". За наявності даного ДВО у абонента, що викликається, викликаючому абонентові не буде представлена інформація про підключений номер.
- переадресація виклику за відсутності відповіді (Call Forwarding No Reply);
- переадресація виклику при зайнятості (Call Forwarding Busy);
- безумовна переадресація виклику (Call Forwarding Unconditional);
- ідентифікація зловмисного виклику (MOD) - дозволяє інформувати оператора зв'язку про зловмисний виклик, що стався;
- індикація чекаючого виклику/повідомлення (Call/Message Waiting) - сповіщення про вхідний дзвінок, коли абонент вже веде розмову (при другому виклику абонент чує звукове сповіщення);

- завершення виклику (Call Completion) - дозволяє викликаючому абонентові А, що зустрів зайнятість абонента В, що викликався, отримати з'єднання з абонентом В, коли останній звільниться, без здійснення повторної спроби виклику. Якщо абонент А зустрічає зайнятість абонента, що викликається, він може активувати дану послугу зі свого телефонного апарату. ДВО контролюватиме абонента, що викликається, з метою визначення моменту часу коли він звільниться. Коли абонент В звільниться і не робитиме повторних спроб виклику протягом певного проміжку часу (зазвичай 10-20 с.), станція підготує комутаційний тракт між абонентами А і В і пошле виклик абонентові А. Коли абонент А відповість на виклик, посилається сигнал виклику абонентові В і далі з'єднання встановлюється звичайним порядком;
- паркування і перехоплення викликів (Call Park/Pick-up) - "паркування" дозволяє ставити вхідні виклики в режим чекання і повертати їх з цього стану в довільній послідовності. «Припаркувавши» вхідний виклик, абонент може, продовжувати працювати з поточним з'єднанням, здійснювати нові виклики зі свого телефону і навіть покласти трубку. Даний сервіс корисний при необхідності реагувати на велику кількість вхідних викликів. Сервіс «Перехоплення дзвінка» дозволяє абонентам приймати виклики, адресовані іншим абонентам Системи. Наприклад, якщо хто-небудь із співробітників відсутній, його колеги можуть відповідати на дзвінки замість нього зі своїх телефонних апаратів.
- утримання виклику (Call Hold) - сервіс дозволяє «ставити» вхідні виклики в режим очікування;
- замкнута група користувачів (CUG) - Забезпечує взаємодію абонентів, що входять до організованої замкнутої групи;
- конференц-зв'язок з розширенням (CONF) та інші.

Слід зазначити, що залежно від використовуваного типа підключення і термінального устаткування, а також від можливостей управляючого вузла (наприклад, Softswitch) список і алгоритми надання послуг можуть відрізнятися. Також слід зазначити, що фрагмент NGN для викликів, що проходять через нього, повинен забезпечувати підтримку ДВО, ініційованих в інших мережах.

Послугами доступу, що підтримуються з боку мережного фрагмента NGN, є:

- послуги доступу в мережі IP по комутованому з'єднанню з підтримкою процедур точки доступу і авторизації з боку фрагмента NGN - застосовуються як для підтримки WWW, e-mail, FTP-застосувань, так і для доступу до мереж IP- телефонії;

- послуги доступу до ресурсів IN з реалізацією функції SSP в мережному фрагменті NGN. SSP повинен як мінімум забезпечувати підтримку наступних видів послуг інтелектуальної мережі:
  - "Безкоштовний виклик";
  - "Телеголосування";
  - "Виклик з додатковою оплатою";
  - "Виклик по передоплаченій карті".
- послуги доступу до інформаційно-довідкових ресурсів з підтримкою точки доступу і авторизації доступу з боку фрагмента NGN.

До інформаційно-довідкових відносяться послуги надання інформації з боку елементів фрагмента NGN. Надання доступу до інформаційно-довідкових ресурсів передбачає включення сервера послуги до складу фрагмента NGN і використання API-інтерфейсів між Softswitch і сервером застосувань.

Фрагментом NGN може підтримуватися надання наступних видів послуг віртуальних приватних мереж:

- віртуальна приватна мережа (VPN) на основі комутованих з'єднань з підтримкою адресного простору VPN з боку Softswitch. В цьому випадку завданням Softswitch є аналіз номера вхідного/вихідного абонента з прийманням рішення про можливість встановлення з'єднання відповідно до політики VPN. Після приймання позитивного рішення про встановлення з'єднання обробляється у фрагменті NGN як звичайний виклик;
- віртуальна приватна мережа на основі постійних з'єднань усередині фрагмента NGN з обробкою адресної інформації з боку гнучкого комутатора. В цьому випадку для віртуальної приватної мережі спочатку резервується транспортний ресурс у фрагменті NGN. Обслуговування викликів VPN здійснюється гнучким комутатором в рамках виділеного для VPN транспортного ресурсу;
- віртуальна приватна мережа на основі постійних з'єднань без обробки сигнальної інформації виклику гнучким комутатором. В цьому випадку VPN використовує фрагмент NGN лише як транспортний ресурс. Обробкою сигнальної інформації, що відноситься до виклику, займаються зовнішні до фрагмента пристрої.

Мультимедійні послуги можна розглядати з двох позицій:

- з позиції абонентів послуг зв'язку;
- з позиції постачальника послуг (оператора зв'язку).

З точки зору абонентів, мультимедійна послуга зв'язку є можливістю мережі забезпечити функціонування специфічних мультимедійних призначених для користувача застосувань. Фактично абонентові байдуже, на базі якої мережі надається мультимедійна послуга, тобто послуга не залежить від технологічної платформи мережі.

Мультимедійний додаток користувача є додатком, що одночасно підтримує декілька "одиниць" представлення аудіовізуальній інформації і надає абонентам загальний інформаційний простір в рамках одного сеансу зв'язку. Як приклади мультимедійних застосувань можна привести наступні: спільна робота з документами і графікою, "біла дошка ", дистанційне навчання, телемедицина і ін.

Оператор зв'язку розглядає мультимедійну послугу зв'язку як перенесення комбінації двох або більш "одиниць" представлення аудіовізуальній інформації (тобто відео, звуку, тексту) між абонентами в рамках мережної інфраструктури і з врахуванням складу і можливостей використовуваного устаткування. Таким чином, можливість надання тієї або іншої мультимедійної послуги повністю залежить від технологічної платформи мережі.

Європейський інститут стандартизації в області зв'язку (ETSI) ввів поняття "Широкосмугових мультимедійних послуг ". Під такими послугами розуміються послуги зв'язки, надання яких здійснюється на базі широкосмугових мереж зв'язку, здатних забезпечити перенесення інформації (контенту) у вигляді безперервних потоків пакетів/чарунок в режимі реального часу."

Класифікацію мультимедійних послуг зв'язку і застосувань можна проводити з різних точок зору і з використанням різних критеріїв.

Як приклад класифікації, що відображає точку зору оператора мережі B-ISDN, можна привести рекомендацію ITU-T I.211. Суть підходу полягає в тому, що послуги зв'язку надаються абонентам за допомогою певних служб B-ISDN. Згідно рекомендації, залежно від способів зв'язку між термінальним устаткуванням абонентів і відповідно до можливих призначених для користувача застосувань всі служби діляться на інтерактивних і розподільних, кожна з яких, у свою чергу, включає декілька класів служб.

Контрольні запитання

1. Назвіть особливості інфокомунікаційної мережі.
2. Сформулюйте основні вимоги до мереж зв’язку
3. Що таке інфокомунікаційна послуга?
4. Визначте особливості інфокомунікаційних послуг в порівнянні з послугами традиційних мереж зв’язку.
5. Сформулюйте зміст і дайте визначення мережі наступного покоління NGN, її базові принципи.
6. Визначте відмінності бізнес-моделі процесу надання інфокомунікаційних послуг від бізнес-моделі надання традиційних послуг електрозв'язку.
7. Який принцип побудови інтелектуальної мережі?
8. Які основні переваги інтелектуальної мережі?
9. Які основні функції вузлів інтелектуальної мережі?
10. Поясніть, чим відрізняється послуга ідентифікації викликаючої лінії від послуги ідентифікації підключеної лінії.

Розділ 2. Архітектура NGN

2.1. Стандартизація NGN

Розробкою нової мережної архітектури NGN і її стандартизацією займаються наступні організації:

- Сектор стандартизації телекомунікацій Міжнародного союзу електрозв'язку (International Telecommunication Union, Telecommunication sector, ITU-T);
- Європейський інститут по стандартизації в області телекомунікацій (European Telecommunications Standards Institute, ETSI);
- Проекти партнерства для створення мереж 3G (3rd Generation Partnership Project 3GPP і 3GPP2);
- Інженерна група підтримки Інтернет (Internet Engineering Task Force, IETF).

У складі цих організацій створені спеціалізовані групи або проекти, діяльність яких направлена на розробку нормативних документів в сфері NGN.

Стандартизація NGN в МСЕ Т

У 2003 році у складі Дослідницької комісії 13 була утворена загальна звітна група по проблемах NGN (Joint RapporteurGroup on NGN — JRG NGN). Основними напрямами її роботи були: вимоги до NGN, загальна описова модель, функціональні вимоги і архітектура NGN, еволюція NGN. Розроблена базова архітектура нормативних документів МСЕ-Т по NGN.

Сьогодні стандартизація NGN визнана одним з пріоритетних напрямів роботи ITU-T. Так, в програму вивчення Дослідницької комісії включені питання:

- принципи і функціональна архітектура NGN;
- вимоги і структура для якості обслуговування в NGN;
- рухливий зв'язок і конвергенція рухливих і фіксованих можливостей в NGN;
- вплив протоколу IP v6 на NGN;
- взаємодія служб і мереж в NGN;
- універсальна мобільність в NGN;
- аспекти обслуговування: можливості послуг і архітектура послуг;
- основні характеристики і вимоги до майбутніх пакетних мереж.

Стандартизація NGN в ETSI

Для координації робіт в ETSI по стандартизація мереж NGN в квітні 2001 року була створена Робоча група NGN SG (Telecoms & Internet converged Services & Protocols for Ad I raiced Networks – TISPAN). У 2003 році в результаті об'єднання двох робочих груп ETSI – групи TIPHON (Telecommunications and Internet Protocol Harmonisation over Net works), що займається гармонізацією телефонних мереж і мереж IP-телефонії, і Технічного комітету SPAN (Services and Protocols for Advanced Networks), що займається питаннями класичних телефонних мереж, була створена нова робоча група TISPAN. Робоча група TISPAN складається з 8 підгруп, кожна з яких вивчає різні аспекти фіксованих мереж наступного покоління: архітектура, елементи рівня управління, елементи рівня послуг, менеджмент, тестування безпеки і так далі (рис. 2.1).

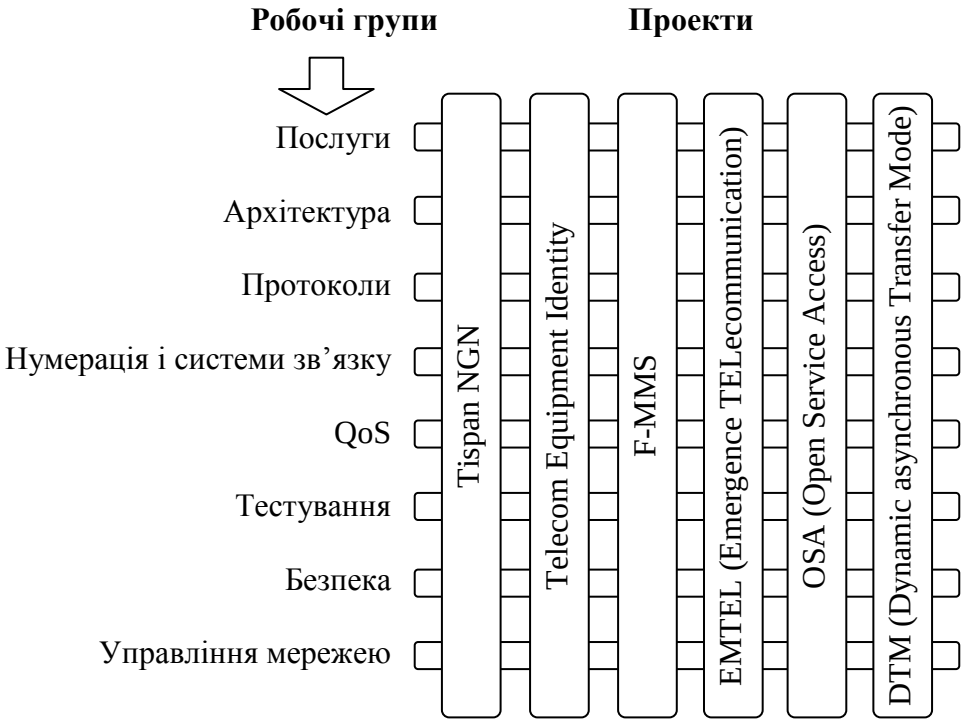


Рис. 2.1. Напрямки робіт і проекти робочих груп TISPAN

У серпні 2005 року група TISPAN опублікувала перші документи, що описують архітектуру мережі NGN. Ця архітектура увібрала в себе напрацювання групи 3GPP. Одним з ключових елементів архітектури є мультимедійна IP-підсистема IMS (IP Multimedia Subsystem). Серед важливих принципів IMS слід зазначити, що вона базується на відкритих стандартах Інтернет і тому без додаткової адаптації може використовувати всі послуги і додатки мережі Інтернет, проте усередині самої IMS передбачено вживання протоколу IPv6. Другою особливістю архітектури IMS є інноваційний підхід до

надання послуг, що дозволяє операторові створювати різні послуги і інтегрувати їх, а також що забезпечує широкі можливості по персоналізації і збільшенню кількості послуг. Використання єдиної архітектури групами TISPAN і 3GPP відкриває дорогу до стандартного вирішення конвергенції сервісних плат форм фіксованої і мобільної мереж зв'язку. Будучи партнером проекту 3GPP, ETSI узяв на себе зобов'язання перетворення специфікацій, що випускаються проектом 3GPP, у тому числі, і по NGN, в ETSI версії.

2.2. Стандартизація підсистеми IMS в межах партнерств 3GPP і 3GPP2

Стандартизація архітектури IMS (IP Multimedia Subsystem) є предметом уваги широкого круга міжнародних організацій, яка визначається ключовою роллю IMS в еволюції мереж у напрямі до NGN. Концепція IMS в її справжньому вигляді є, головним чином, результатом робіт трьох міжнародних організацій з стандартизації – 3GPP, 3GPP2 і ETSI. Партнерство 3GPP було створене в кінці 1998 р. за ініціативою інституту ETSI з метою розробки технічних специфікацій і стандартів для мобільних мереж зв'язку 3G (мереж UMTS), що базуються на мережах GSM в процесі їхнього розвитку. Партнерство 3GPP2 з'явилося в 1998 р. також за ініціативою ETSI і Міжнародного союзу електрозв'язку для розробки стандартів мереж 3G (мережі cdma2000) в рамках проекту IMT 2000, створеного під егідою МСЕ. Обидва партнерства розробляють стандарти мереж 3G, орієнтуючись на широке вживання IP орієнтованих протоколів, стандартизованих Комітетом IETF, і використовуючи основні ідеї архітектури мереж NGN.

Вперше концепція IMS була представлена в документі 3GPP Release 5 (березень 2002 р.). У ньому була сформульована основна її мета – підтримка мультимедійних послуг в мобільних мережах на базі протоколу IP і специфіковані механізми взаємодії мобільних мереж 3G на базі архітектури IMS з безпроводовими мережами 2G.

Архітектура мереж 3G відповідно до концепції IMS має декілька рівнів (площин) з розділенням за рівнями транспорту, управління викликами і застосувань Підсистема IMS має бути повністю незалежна від технологій доступу і забезпечувати взаємодію зі всіма існуючими мережами – мобільними і стаціонарними, телефонними, комп'ютерними і так далі. У документі 3GPP Release 6 ряд положень концепції IMS було уточнено, додано питання взаємодії з безпроводовими локальними мережами і захисту інформації: використання ключів, абонентських сертифікатів.

У специфікації, яка розроблялася ETSI спільно з Комітетом TISPAN, розглядається взаємодія мобільних і стаціонарних мереж, тобто зроблено перший реальний крок у напрямі конвергенції стаціонарних і мобільних мереж. Специфікація Release 7 додає дві основні функції, які є ключовими в стаціонарних мережах:

- функція підключення до мережі (Network Attachment), яка забезпечує механізм аутентифікації абонентів і необхідна в стаціонарних мережах, оскільки в них відсутні SIM карти ідентифікації користувача;
- функція доступу до ресурсів (Resource Admission), що резервує мережні ресурси в стаціонарних мережах для забезпечення сеансів зв'язку.

2.3. Архітектура NGN за чотирьохрівневою моделлю

З розвитком інфокомунікаційних послуг стали вельми популярні обговорення різних варіантів архітектури NGN, яка в рамках єдиної інфраструктури об'єднує мережі ТФЗК, мобільний зв'язок, ресурси мережі Інтернет, телефонію по IP-протоколу. Однією з основних відмінностей концепції NGN від тих мережних інфраструктур, що реалізовувались до цього є перехід до принципово іншої функціональної моделі. У класичній ТФЗК основними функціональними елементами були вузли доступу і вузли комутації різного рівня. При цьому устаткування вузла комутації вирішувало одночасно декілька завдань: комутацію потоків призначеної для користувача інформації, обробку виклику і надання послуг. Реалізація інтерфейсів між цими функціями була внутрішньою справою виробника системи комутації і не підлягала регламентації. Розвиток класичної ТФЗК, пов'язаний, перш за все, з появою технології ISDN, дозволил декілька розділити функції обробки сигналізації і комутації потоків призначеної для користувача інформації.

Концепція NGN, в першу чергу, характеризується чітким розділенням трьох рівнів з'єднання відповідно до їх функціональних завдань: для комутації і передачі мовної інформації використовується транспортний функціональний рівень, для передачі інформації сигналізації - рівень сигналізації, а для надання послуг, відмінних від базових, - рівень послуг. При цьому між рівнями визначені інтерфейси, які є об'єктом стандартизації. Отримавши подібну незалежність друг від друга, рівні надалі можуть розвиватися самостійно. Більш того, з точки зору адміністративного розподілу мережі може ставитися питання про те, аби послуги різних рівнів надавалися різними операторами.

В даний час найбільшого поширення набула чотирьохрівнева (площинна) архітектура NGN:

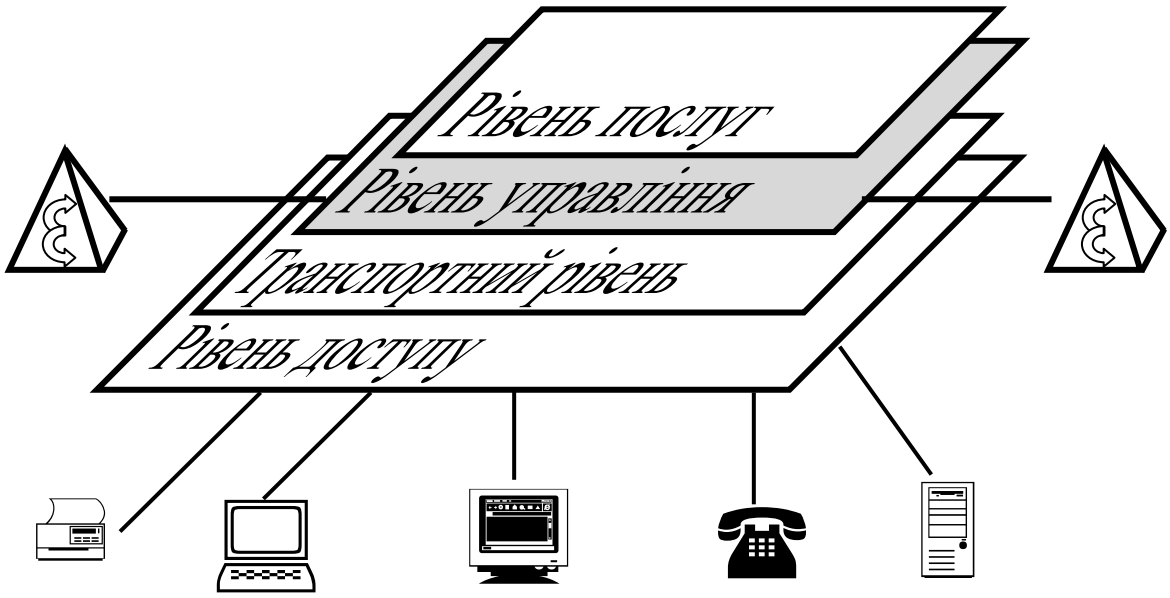


Рис.2.2. Архітектура мережі наступного покоління

Площинна архітектура – базовий принцип NGN, вона дозволить підвищити ефективність операторської діяльності і надати відкриті інтерфейси стороннім розробникам.

Рекомендація МСЕ-Т Y.2011 «Базова архітектура мереж наступного покоління NGN» включає 4 основних функціональних рівня:

- рівень доступу, що містить мережу абонентського доступу до транспортної пакетної мережі;
- транспортний рівень, що включає магістральну мережу, побудовану на базі протоколів пакетної комутації;
- рівень управління викликами (комутацією) включає сукупність функцій з управління всіма процесами в телекомунікаційній мережі. У всіх версіях еталонної архітектури NGN присутній деякий елемент управління, який може називатися гнучким комутатором (Softswitch), вузлом (сервером) управління обслуговуванням викликів, телефонним сервером, Call-агентом або контролером медіашлюзів MGC. Цей елемент забезпечує функції маршрутизації і обслуговування викликів, логіку деяких додаткових послуг і взаємодію із додатками для виконання послуг, обробку сигналізації і управління терміналами при ініціації, переадресації і термінації викликів, а також формує необхідну інформацію для білінга;
- рівень послуг і експлуатаційного управління, який містить логіку виконання послуг і застосувань і управляє цими послугами, має

відкриті інтерфейси для використання сторонніми організаціями (для розробки програм і нових послуг).

Розглянемо детальніше рівні архітектури NGN.

2.3.1. Рівень доступу

Рівень доступу забезпечує підключення користувачів (приватних абонентів, підприємств, мобільних користувачів) до мережі. Залежно від використовуваної технології (xDSL, Ethernet, PON, Cable, Wi-Fi, WIMAX, LTE) вибирається устаткування: DSLAM, комутатори Ethernet, точки доступу Wi-Fi, базові станції WIMAX та ін. Для забезпечення абонентів високоякісними мультимедійними послугами мережі доступу мають бути високошвидкісними, мультисервисными, інтелектуальними, мати високу надійність і доступність.

Особлива увага приділяється інтеграції мереж фіксованого і мобільного доступу, на основі яких має бути забезпечена мобільність абонента. У ідеалі в NGN мережі у кожного абонента має бути наскрізна ідентифікація у всіх сегментах доступу і єдиний абонентський профіль, для чого необхідна єдина система обліку і білінга. Медіашлюзи, встановлені на межі NGN і традиційної ТФЗК, стикують VoIP середовище і лінії TDM.

Одному з важливих завдань, які вирішуються на цьому рівні, є організація взаємодії між мережами з комутацією каналів, що використовують часове мультиплексування і пакетними мережами. Як відомо обоє технології мають свої недоліки і свої достоїнства.

Достоїнства комутації каналів:

- Постійна і відома швидкість передачі даних по встановленому між кінцевими вузлами каналу. Це надає можливість визначити заздалегідь необхідну для якісної передачі даних пропускну спроможність каналу і гарантувати цю пропускну спроможність впродовж всього сеансу зв'язку.

- Низький і постійний рівень затримки передачі даних через мережу. Це дозволяє якісно передавати дані, чутливі до затримок (звані також трафіком реального часу), – голос, відео, різну технологічну інформацію.

- Відсутність необхідності в передачі службової інформації після встановлення з'єднання.

- Комутація каналів може використовуватися як в аналогових, так і в цифрових мережах зв'язку, на відміну від комутації пакетів, яка можлива лише в цифрових мережах.

Недоліки комутації каналів

- Відмова мережі в обслуговуванні запиту на встановлення з'єднання.

- Нераціональне використання пропускної спроможності фізичних каналів. Та частина пропускної спроможності, яка відводиться складеному каналу після встановлення з'єднання, надається йому на весь час, тобто до тих пір, поки з'єднання не буде розірвано. Проте абонентам не завжди потрібна пропускна спроможність каналу під час з'єднання, наприклад в телефонній розмові можуть бути паузи, ще більш нерівномірною в часі є взаємодія комп'ютерів. Неможливість динамічного перерозподілу пропускної спроможності є принциповим обмеженням мережі з комутацією каналів, оскільки одиницею комутації тут є інформаційний потік в цілому.

Достоїнства комутації пакетів:

- Висока загальна пропускна спроможність мережі при передачі пульсуючого трафіку.
- Можливість динамічно перерозподіляти пропускну спроможність фізичних каналів зв'язку між абонентами відповідно до реальних потреб їх трафіку.

Недоліки комутації пакетів:

- Невизначеність швидкості передачі даних між абонентами мережі, обумовлена тим, що затримки в чергах буферів комутаторів мережі залежать від загального завантаження мережі.
- Змінна величина затримки пакетів даних (джитер), яка може бути достатнє тривалою в моменти миттєвих перевантажень мережі.
- Можливі втрати даних із-за переповнювання буферів.

Основна проблематика цього рівня пов'язана з недоліками властивими пакетної мережі (нерівномірні затримки із-за черг, асинхронність передачі даних і, як наслідок, джитер, відсутність гарантованої смуги пропускання для всіх потоків). Припустимо і якості технології доступу використовується SDH (на базі якої, наприклад, побудована корпоративна мережа). Точка доступу між мережею SDH і опорною пакетною мережею повинна реалізовувати перетворення інформаційних потоків з часовим розділенням в пакети. При цьому виникають складнощі з організацією динамічної маршрутизації, оскільки рішення задачі сполучення віртуального каналу SDH з маршрутом IP має жорстко закріплений статичний характер. Друга проблема пов'язана з тим, що необхідно погоджувати параметри надійності мережі і якості послуг, що надаються мережею за технологією SDH, з пакетною мережею (імовірність втрат пакету і бітова помилка, джитер, затримка). Розглянемо модемне з'єднання по протоколу V.90 (56 кБит/с) між абонентами через пакетну мережу, де як адресат використовується телефонний номер ТФЗК. Шлюз, що виконує функції доступу

в пакетну мережу, повинен виділити сигнальну інформацію і на її основі визначити маршрут до абонента, що викликається, реалізовуючи при цьому функцію встановлення з'єднання. Шлюз як точка доступу отримує інформацію від модему у форматі, що передбачається характеристиками модему (аналогова модуляція, наприклад, по протоколу Z-modem або Kermit), перетворює її у формат пакетної мережі (IP/MPLS) і погоджує параметри якості сформованого пакету з параметрами вихідного протоколу.

2.3.2. Рівень транспорту

Транспортний рівень мережі NGN забезпечує створення повнозв'язаної інфраструктури для пакетної передачі даних різного типа з реалізацією підтримки заданої якості обслуговування (QoS).

Транспортний рівень відповідає за прозору передачу інформації користувача різного виду (голос, відео, дані). Причому обмін інформацією між джерелом і пунктом призначення здійснюється поодинці і тому ж принципу незалежно від виду з'єднання (телефонний виклик, сеанс роботи в мережі Інтернет, передача відео, мережна гра з декількома гравцями або трансляція фільму). При цьому як транспортна технологія передачі може використовуватися мультиплексування з розділенням за часом (TDM), асинхронний режим передачі (ATM) або Інтернет-протокол (IP). Проте ефективність використання смуги пропускання, характерна для мереж з комутацією пакетів, приводить до того, що в мережах нового покоління використовуватимуться в основному пакетні технології, такі як IP/MPLS.

Фундаментом NGN є мультипротокольна/мультисервісна транспортна мережа зв'язку на основі пакетної передачі даних, що забезпечує перенесення різнорідного трафіку з використанням різних протоколів передачі.

На даний момент основними мережевими транспортними технологіями є:

1). *Цифрова синхронна ієрархія SDH* - технологія, що базуються на принципах часового мультиплексування. Для існуючих систем синхронної транспортної ієрархії SDH стандартизовані швидкості передачі від STM-1 (155 Мбіт/с) до STM-256 (40 Гбіт/с), що збільшуються від рівня до рівня з коефіцієнтом 4.

В даний час витісняються:

- на електричному рівні – технологіями Carrier Ethernet (інтерфейси E/FE, GE, 10GE, 40GE і 100GE) і MPLS-Transport Profile. Ці технології забезпечать широкі можливості для створення транспортних мереж з пакетною комутацією операторського класу, орієнтованих на встановлення з'єднань;

- на оптичному рівні – технологіями оптичної транспортної ієрархії OTH (Optical Transport Hierarchy), схожими на SDH, але на відміну від неї вони забезпечують прозорість передачі і крос-комутації сукупності TDM- і пакетного трафіку в будь-якому поєднанні з подальшою їх передачею по каналах систем з розділенням каналів за довжиною хвилі (WDM, Wavelength Division Multiplexing – спектральне ущільнення каналів).

2). *Оптичні транспортні мережі (Optical Transport Network – OTN)* будуються з набору оптичних мережних елементів, сполучених оптоволоконними каналами, здатними забезпечити такі функції, як транспорт, мультиплексування, маршрутизація, управління, контроль і живучість каналів, по яких передаються сигнали. Використовує устаткування - мультиплексори введення-виводу (TDM), які можуть містити в своєму складі устаткування мультиплексування по довжині хвилі xWDM.

Відмінною характеристикою OTN є її здатність транспортувати будь-який цифровий сигнал незалежно від специфіки клієнта. У OTN, як і в SDH, визначена ієрархія мережі, звана ієрархією оптичної передачі (Optical Transport Hierarchy – OTH).

Оптична транспортна ієрархія (Optical Transport Hierarchy, OTH), як визначено в Рекомендаціях ITU-T G.709, G.798, передбачає методи розміщення, мультиплексування і управління мережами, що підтримують різні клієнтські сигнали в їх натуральному форматі, незалежно від типів використовуваних протоколів. У стандарті описана єдина структура Optical Data Unit (ODU), в якій можна розмістити декілька існуючих фреймів потоків даних, а потім об'єднати їх з іншими сигналами і далі передавати і управляти в єдиному стилі з єдиною функціональністю, аналогічною тій, що прийнята в системах SDH.

Перша версія OTH була орієнтована переважно на клієнтські сигнали SDH. Тому спочатку в рекомендації G.709 були визначені лише 3 фіксованих типа ODU-контейнеров: ODU1, відповідний рівню STM-16 технології SDH, ODU2, відповідний рівню STM-64 і ODU3, відповідний рівню STM-256.

В даний час структури OTH розглядаються з врахуванням передачі таких сигналів, як:

Ethernet 1GE, 10GE WAN/LAN, 40GE, 100GE;

OTH 2,5G, 10G, 40G, 100G;

SDH 2,5G, 10G, 40G;

FC 1G, 2G, 4G, 8G (10G).

Технологія OTN може використовуватися для створення конвергентних транспортних платформ, що забезпечують прозорість при передачі трафіку, що відноситься до будь-яких послуг поверх оптичних каналів WDM-систем, оскільки має власний окремий заголовок, схожий на заголовок в SDH і, що дає

можливість контролювати мережу і управляти нею. Це дозволяє підтримувати прозору спільну передачу сукупності асинхронного (пакетного) і синхронного (TDM) трафіку в будь-яких поєднаннях.

3). *Технологія MPLS* - «багатопротокольна комутація з використанням міток» (Multiprotocol Label Switching) - обєднує технології комутації другого рівня з технологіями маршрутизації третього рівня (поєднує в собі можливості управління трафіком, властиві технологіям канального рівня, і масштабованість і гнучкість протоколів, характерні для мережного рівня). Головна особливість технології MPLS – відділення процесу комутації пакету від аналізу IP-адреса в його заголовку, що дозволяє здійснювати комутацію пакетів значно швидше приводить до зростання продуктивності мережі. MPLS є масштабованим і незалежним від яких-небудь протоколів механізмом передачі даних. У мережі, заснованій на MPLS, пакетам даних привласнюються мітки. Вирішення про подальшу передачу пакету даних іншому вузлу мережі здійснюється лише на підставі значення привласненої мітки без необхідності вивчення самого пакету даних. За рахунок цього можливе створення наскрізного віртуального каналу, незалежного від середовища передачі і який використовує будь-який протокол передачі даних. Основною перевагою MPLS є незалежність від особливостей технологій канального рівня, таких як ATM, Frame Relay, SONET/SDH або Ethernet, і відсутність необхідності підтримки декількох мереж другого рівня, необхідних для передачі різного роду трафіку. По виду комутації MPLS відноситься до мереж з комутацією пакетів.

4). *Технологія Carrier Ethernet* (інтерфейси E/FE, GE, 10GE, 40GE і 100GE) дозволяє використовувати достоїнства технології Ethernet в мережах операторського класу (невисока вартість і легка масштабованість). Підтримується QOS, тунелювання трафіку, передача широкомовних повідомлень. Carrier Ethernet надає наступні три типа стандартизованих сервисів: E- Line: сервіс, що емулює віртуальне виділене з'єднання точка – точка через мережу Carrier Ethernet; E – LAN: сервіс, що емулює користувачеві з'єднання LAN через Carrier Ethernet мережу; E - Tree: сервіс, що емулює передачу мультикастингового трафіку

Для існуючих систем синхронної транспортної ієрархії SDH стандартизовані швидкості передачі від STM-1 (155 Мбіт/с) до STM-256 (40 Гбіт/с), що збільшуються від рівня до рівня з коефіцієнтом 4. Для систем оптичної транспортної ієрархії стандартизовані швидкості передачі від OTU-1 (2,5/2,7 Гбіт/с) до OTU-3 (40/43 Гбіт/с), які також збільшуються від рівня до рівня з коефіцієнтом 4. Швидкість передачі Ethernet зростала з коефіцієнтом 10 і досягла на сьогоднішній день 100 Гбіт/с. Конвергенція цих технологій почалася

з швидкостей передачі 10G. Дослідження останніх років показали, що ця конвергенція розвивається у напрямі швидкостей передачі 40 Гбіт/с і 100 Гбіт/с.

Задоволення поставлених сервіс-провайдерами вимог неможливе без освоєння швидкостей передачі даних в діапазоні до 100 Гбіт/с і вище.

Розглянемо модель побудови транспортної мережі NGN відповідно до моделі взаємодії відкритих систем OSI - на різних рівнях працюють різні процеси і використовуються різні технології.

Фізичний рівень представлений волоконно-оптичними системами передачі (ВОСП) на основі волоконно-оптичних ліній зв'язку (ВОЛЗ). Поверх нього розміщується устаткування оптичного мультиплексування (WDM/DWDM), Вище за рівень WDM знаходяться системи оптичної комутації, де за допомогою спеціальних пристроїв оптичний сигнал комутується і надалі поширюється по іншому волокну або в іншому діапазоні хвиль без аналогово-цифрових перетворень, оскільки тут дані передаються безпосередньо у вигляді цифрового сигналу.

Основною технологією фізичного рівня мають бути ВОСП. Сучасні вимоги по передачі парного трафіку орієнтовані на швидкість передачі даних більше 10 Гбіт/с. Таку швидкість передами може забезпечити лише волоконно-оптична технологія, тобто ВОСП.

Технологія WDM/DWDM оптимізує використання оптичних кабелів за рахунок системи спектрального мультиплексування, що дозволяє формувати декілька цифрових каналів широкосмугової передачі на одному оптичному волокні. Системи оптичної комутації доповнюють цю систему, забезпечуючи комутацію сигналів з однієї довжини хвилі на іншу.

На фізичному рівні має місце поліваріантністъ технічних рішень. Оператор в рівній мірі може використовувати лише системи передачі на основі ВОЛЗ, ВОСП з системами WDM і оптичною комутацією.

На канальному рівні транспортних мереж застосовуються різні технології, які дозволяють завантажити дані по протоколу IP у ВОСП на фізичному рівні. Як можливі варіанти можуть застосовуватися технології MPLS, мережі Ethernet і Gigabit Ethernet (GE), вже розгорнуті мережі ATM і Frame Relay, а також стек технологій систем зберігання інформації (SAN), куди входять технології Fiber Channel, FICOX, ESCON. Окрім перерахованих технологій допускається і варіант прямого завантаження дейтаграм IP у ВОСП.

Всі рішення об'єднуються на мережному рівні, який включає два підрівні. На нижньому підрівні дані від різних систем канального рівня перетворяться в дейтаграми єдиного формату IP, верхній підрівень об'єднує різні рішення в частині організації маршрутизації отриманих дейтаграмм.

Завершує модель транспортний рівень, де дейтаграми IP збираються в кадри TCP або UDP, які власне і передаються по транспортній мережі.

Не існує чіткого розподілу технічних рішень за рівнями OSI: деякі технології виконують функції одночасно декількох рівнів, інші - лише окремих рівнів або навіть підрівнів. Можна об'єднати різні варіанти рішень на фізичному і канальному рівні, як вирішення підрівня опорних мереж, який включає технології ВОЛЗ, WDM, оптичної комутації і магістрального Ethernet. Вище за цей підрівень доцільно ввести підрівень пакетної комутації, до якого відноситься MPLS. Над ним розмістимо підрівень маршрутизації, а вище виділимо підрівень транспортної мережі, який вже повністю відповідає транспортному рівню моделі OSI.

Таким чином, можна виділити декілька різних методів завантаження даних комутованого IP у ВОСП:

IP → MPLS → WDM → ВОСП
IP → Ethernet → ВОСП;
IP → Ethernet → WDM → ВОСП;
IP → Оптична комутація → WDM → ВОСП;
IP → WDM → ВОСП;
IP → ВОСП.

Можна сформулювати наступні вимоги, яким повинна відповідати сучасна транспортна пакетна мережа. Транспортна пакетна мережа - це така мережна архітектура, яка має наступні характеристики:

1) розміщується нижче за рівень IP-послуг і вище за рівень фізичного середовища передачі оптичної транспортної мережі. Ця архітектура розробляється відповідно до вимог, що пред'являються до корисного навантаження пакетної мережі і до статистичного мультиплексування;

2) ядро мережі дозволяє надавати мультисервісні послуги;

3) забезпечує традиційні переваги оптичної передачі, у тому числі: доступність і відмовостійкість; ефективний механізм управління пропускною спроможністю і трафіком, а також масштабованість;

Проводячи порівняння між мережами, що базуються на технології часового розділення каналів, і мережами з комутацією пакетів, необхідно відзначити наступне.

Традиційні мережі, засновані на синхронній цифровій ієрархії, мають високу вартість, і низьку адаптивність. Висока вартість устаткування SDH і його обслуговування є істотними недоліками даної технології. Тим часом, пакетні мережі, неорієнтовані на з'єднання в змозі гарантувати задану якість деяких

послуг. Технологія часового мультиплексування непридатна для надання мультисервісних послуг із-за її низької ефективності.

Проте, формування транспортних мереж нового покоління на базі пакетних технологій створюють ряд серйозних проблем. Основою даних проблем є протиріччя між необхідністю дотримання чіткої черговості при передачі потокових повідомлень і базовим принципом пакетної технології, що полягає в недотриманні черговості при отриманні пакетів. Таким чином, стає актуальним рішення задачі забезпечення передачі даних в мережах з комутацією пакетів з тією ж якістю, яку забезпечують мережі цифрової синхронної ієрархії. Це фактично означає необхідність емуляції синхронного комутованого каналу мережею з комутацією пакетів.

2.3.3. Рівень управління викликами (комутацією)

Завдання рівня управління комутацією - обробка інформації сигналізації, маршрутизація викликів і управління потоками. Даний рівень підтримує логіку управління, яка необхідна для обробки і маршрутизації трафіку.

На цьому рівні виконуються наступні функції:

- обробка всіх видів сигналізації, використовуваних в домені управляючого вузла;
- зберігання і управління абонентськими даними користувачів, що підключаються до домена управляючого вузла (програмний комутатор Softswitch, контролер медіашлюзів MGC), безпосередньо або через обладнання шлюзів доступу;
- взаємодія з серверами застосувань для надання розширеного списку послуг користувачам мережі.

В даний час існують дві базові платформи, на яких реалізується цей рівень:

- рішення на базі гнучкого (програмного) комутатора (Softswitch);
- рішення на базі мультимедійної IP-підсистеми (IMS).

Ці рішення мають свої переваги і недоліки. Одній з сильних сторін підходу на базі гнучкого комутатора в даний час є його поширеність: в світі існує множина мереж, що пішли по цій дорозі розвитку, вже накопичений великий дослідний матеріал по впровадженню Softswitch архітектури. Проте в рішення на базі гнучкого комутатора є і недоліки. Різноманіття представленого в даному сегменті ринку устаткування породжує проблему його сумісності.

Деякі виробники устаткування надають фірмові системи управління мережею, які не завжди коректно і повноцінно працюють з устаткуванням сторонніх постачальників при його інтеграції в мережу оператора, оскільки є відмінності не тільки в реалізації, але і у функціональності багатьох систем.

Підхід на базі підсистеми IMS вигідно відрізняється наявністю стандартів, які дають можливість мати одноманітні і тому здатні ефективно взаємодіяти мережі. При цьому частково згладжуються проблеми сумісності устаткування, оскільки взаємодія функціональних модулів регулюється стандартами.

Такі підходи, по суті, мають одну і ту ж рівневу структуру. Як в одному, так і в іншому випадку необхідний єдиний мультисервісний абонентський доступ і єдиний IP-транспорт, акцент робиться на послуги для абонента, тому оператор при виборі стратегії побудови NGN повинен виходити, перш за все, з планованого набору послуг.

2.3.4. Рівень послуг (додатків)

Рівень послуг містить функції управління логікою послуг і застосувань і є розподіленим обчислювальним середовищем, що забезпечує:

- надання інфокомунікаційних послуг;
- управління послугами;
- створення і впровадження нових послуг;
- взаємодія різних послуг.

Даний рівень дозволяє реалізувати специфіку послуг і застосовувати одну і ту ж програму логіки послуг незалежно від типа транспортної мережі і способу доступу. Наявність цього рівня дозволяє також вводити на мережі електрозв'язку будь-які нові послуги без втручання у функціонування інших рівнів.

Рівень послуг може включати множину незалежних підсистем ("мереж послуг "), що базуються на різних технологіях, що мають своїх абонентів і що використовують свої, внутрішні системи адресації. Операторам зв'язку потрібні механізми, що дозволяють швидко і гнучко розгортати, а також змінювати послуги залежно від індивідуальних потреб користувачів.

Такі механізми передбачені відкритою сервісною архітектурою OSA (Open Services Access) – основною концепцією майбутнього розвитку мереж електрозв'язку в частині впровадження і надання нових додаткових послуг.

При створенні систем на основі OSA мають бути присутніми наступні ключові моменти:

- відкрите середовище для створення послуг;
- відкрита платформа управління послугами.

Розглянемо детальніше варіанти архітектури NGN, які запропоновано різними організаціями.

2.4. Архітектура NGN за концепцією ITU-T

Однією з головних характеристик мережі NGN є розділення функціональності послуг і транспорту, що дозволяє розвивати сервіси управління послугами, транспортні і прикладні сервіси незалежно один від одного. Розділення представляється у вигляді двох функціональних рівнів. Транспортні функції відносяться до транспортного рівня, а функціональність послуг лежить, відповідно, на рівні послуг. Горизонтальне розшарування показано на рис. 2.3, а вертикальне - на рис. 2.4. Відзначимо наступні особливості такого розшарування.

Транспортний рівень може складатися з набору різних площин, що відносяться до трьох нижніх рівнів еталонної моделі взаємодії відкритих систем (OSI/MBBC). Таким чином, транспортні функції надають можливість з'єднання двох мереж різної архітектури.

Як показано на рис.2.3, на транспортному рівні можуть бути реалізовані будь-які існуючі мережні технології, включаючи передачу даних з комутацією каналів (Connection Oriented Circuit Switched, CO-CS), передачу даних з комутацією пакетів (Connection Oriented Packet Switched, CO-PS) і пакетну передачу інформації без встановлення з'єднання (Connectionless Packet Switched, CLPS) згідно Рекомендаціям MCE-T G.805 і G.809. Передбачається, що протокол IP буде базовим протоколом в NGN для надання як нових, так і по можливості існуючих послуг.

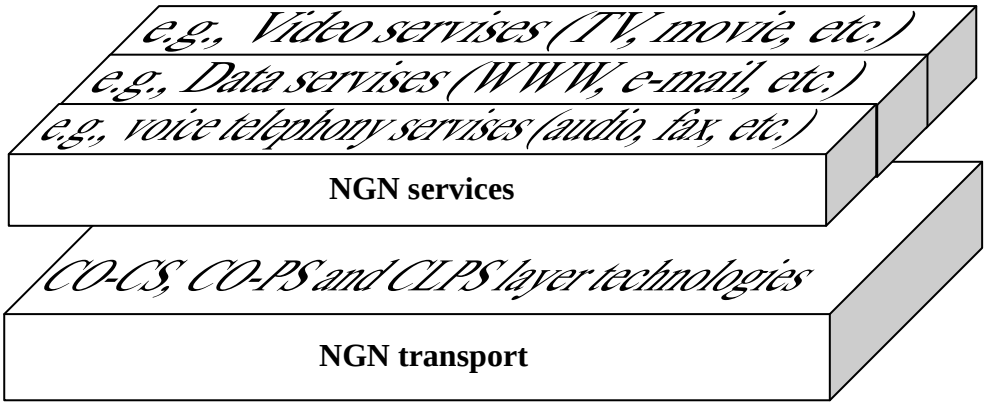


Рис.2.3. Розподіл функціональності послуг і транспорту

Існує набір прикладних функцій, необхідних для надання послуг. До таких послуг відносяться голосові послуги (включаючи телефонію), послуги з передачі даних (включаючи Web-послуги), відеопослуги (включаючи перегляд фільмів і телевизійних програм) або комбінація вищеперерахованих послуг (наприклад, мультимедійні послуги, такі як відеотелефонія або ігри). На рис. 2.3 наведено приклади послуг мереж наступного покоління.

З іншого боку, як показано на рис. 2.4, кожен рівень містить декілька шарів, кожен з яких називається площина даних або площина користувача, площина контролю і площина управління. Така модель називається базовою еталонною моделлю NGN.

Площини даних користувача, управління і менеджменту логічно завжди присутні в кожному шарі. Проте, на практиці для деяких шарів можуть бути відсутніми площини управління або менеджменту. Функції, ідентичні функціям площини контролю і управління в багатошаровій архітектурі, можуть бути реалізовані в одному єдиному протоколі. Це стосується, наприклад, таких технологій, як оптична мережа з автоматичною комутацією (Automatically Switched Optical Network, ASON) і узагальнена мультипротокольна комутація по мітках (Generalized Multiprotocol Label Switching. GMPLS).

Таким чином, площину управління в NGN можна розглядати як сукупність площини управління рівня послуг і площини управління транспортного рівня а площину контролю – як сукупність площини контролю рівня послуг і площини контролю транспортного рівня.

Важливо відзначити, що концепція площин NGN не передбачає вертикальну інтеграцію площин, але вимагає наявності точок зіткнення між ідентичними площинами різних рівнів. Дана концепція необхідна для спрощення переходу від функціонального розгляду побудови мережі NGN до її практичної реалізації.

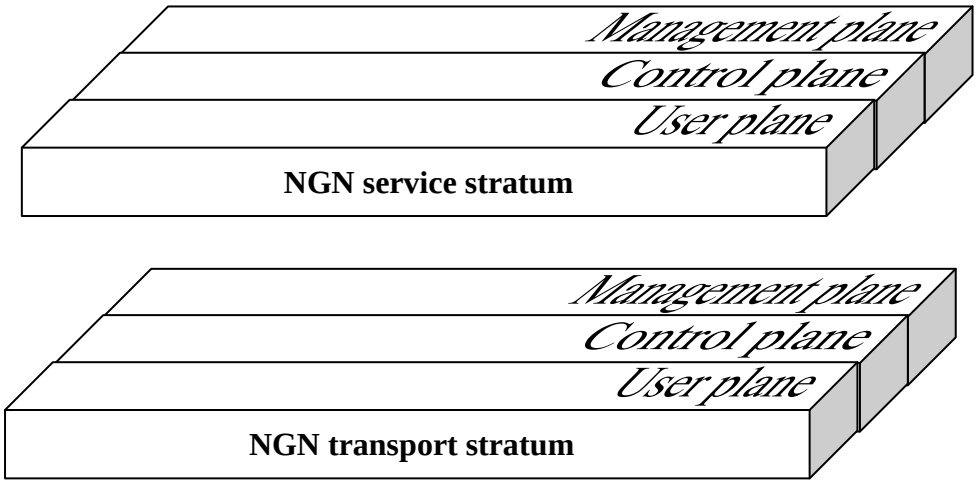


Рис. 2.4 – Базова еталонна модель NGN

До функцій контролю на рівні послуг можна віднести ідентифікацію і аутентифікацію користувача, управління доступом до послуг тощо, а до функцій контролю на транспортному рівні відносяться управління доступом до мережі, контроль мережних ресурсів.

Функції і процеси, що відносяться до площини управління на рівні послуг, описані в серії Рекомендацій ITU-T M.3050.xx. Функції управління мережею на транспортному рівні базуються на концепції TMN, описані в Рекомендації M.3400 і класифіковані за наступними функціональними сферами:

- управління при відмовах;
- управління конфігурацією;
- управлінням розрахунками;
- управління продуктивністю;
- управління безпекою.

Рівень управління послугами повинен застосовувати одну і ту ж програму логіки послуги незалежно від типа транспортної мережі (IP, ATM, FR і тому подібне) і способу доступу. Наявність цього рівня дозволяє також вводити на мережі будь-які нові послуги без втручання в функціонування інших рівнів. Рівень управління послугами може включати множину незалежних підсистем («мереж послуг»), що базуються на різних технологіях і мають своїх абонентів і що використовують свої внутрішні системи адресації.

2.5. Архітектура NGN за концепцією 3GPP

IP Multimedia Subsystem (IMS) — сервісна мультимедійна IP-система – загальна технологічна інфраструктура, що допомагає об'єднати засоби передачі голосового і мультимедійного трафіку в рамках єдиної мультисервісної платформи. Як транспортна інфраструктура передбачається пакетна мережа на базі IP/MPLS (або будь-якій мережі IP)

IMS визначає стандартну базову архітектуру для надання послуг передачі голосу (VoIP) і мультимедіа на основі розробленого 3GPP варіанту протоколу SIP.

Метою створення IMS було забезпечення умов для впровадження мультимедійних послуг разом з розвиненими функціями управління для операторів мереж NGN, а для операторів мобільних мереж – забезпечення умов для надання послуг на базі IP. Версія IMS (3GPP R.5) передбачає підтримку мереж GSM/GPRS (2G) і WCDMA/UMTS (3G). У версії від 3GPP2 додана підтримка WLAN і cdma2000, мультимедійних послуг реального часу MMD. Версії 3GPP R.6, R.7 і R.8 націлені на конвергенцію мобільних і фіксованих мереж (Fixed Mobile Convergence, FMC).

По суті, концепція IMS виникла в результаті еволюції мереж UMTS, коли сферу управління мультимедійними викликами і сеансами на базі протоколу SIP додали до архітектури мереж 3G. Серед основних властивостей архітектури IMS можна виділити наступні:

- багаторівневість – розділяє рівні транспорту, управління і застосувань;
- незалежність від середовища доступу – дозволяє операторам і сервіс-провайдерам здійснювати конвергенцію фіксованої і мобільної мереж;
- підтримка мультимедійного персонального обміну інформацією в реальному часі і аналогічного обміну інформацією між людьми і комп'ютерами (наприклад, ігри);
- повна інтеграція мультимедійних застосувань реального і нереального часу (наприклад, потокові додатки і чати);
- можливість взаємодії різних видів послуг;
- можливість підтримки декількох служб в одному сеансі або організації декількох одночасних синхронізованих сеансів.

Наявність таких елементів IMS, як база даних абонентів (Home Subscriber Server – HSS), де міститься також інформація про кінцеве устаткування, і контроллери медіашлюзів (Media Gateway Contrail Function, MGCF), спрощує адаптацію послуг для різних абонентських пристроїв і надання уніфікованих послуг.

Розглянемо архітектуру IMS детальніше. На рис. 2.5 показана мережа, що має багаторівневу архітектуру, яка включає три рівні: транспортний, управління і послуг. Підсистема мультимедійного зв'язку розташована на рівні управління, який є основним в архітектурі IMS.

Вузол обслуговування абонентів GPRS (Serving GPRS Support Node, SGSN) – основний компонент GPRS-системи з реалізації всіх функцій обробки пакетної інформації.

SGSN містить всі параметри мобільних абонентів GPRS, потрібні для пакетної передачі і виконує наступні функції:

- управління сеансом;
- функції, що відносяться до сеансу пакетного зв'язку;
- управління мобільністю;
- управління ресурсами;
- обробка (диспетчеризація) пакетів.

Новим ключовим елементом в архітектурі IMS є функція управління викликами і сеансами CSCF (Call Session Control Function). Функція CSCF є основною на площині управління IMS-платформи. Модуль CSCF, використовуючи протокол SIP, виконує функції, що забезпечують доставку

множини послуг реального часу за допомогою протоколу IP. Модуль CSCF включає три основні функції: обслуговуюча CSCF (Serving CSCF, S-CSCF), CSCF доступу (Proxy CSCF, P-CSCF), і запитуюча CSCF (Interrogating CSCF, I-CSCF).

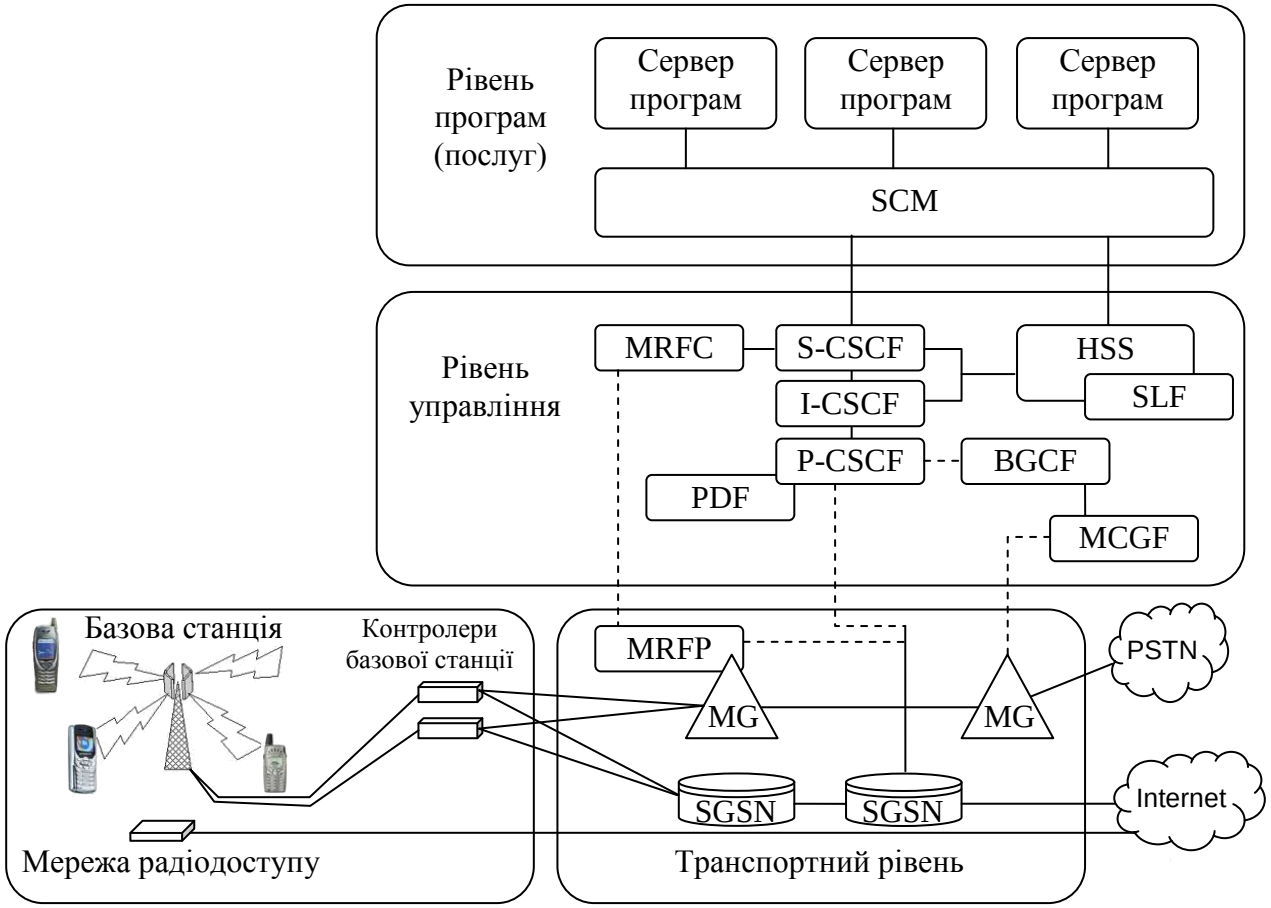


Рис. 2.5. Архітектура підсистеми IMS

Порівняємо основні підходи до побудови мереж NGN. Фактично в даний час існують два основні підходи до побудови мереж NGN:

- рішення на базі гнучкого комутатора (Softswitch);
- рішення на базі мультимедійної IP-підсистеми (IMS).

Ці рішення мають свої переваги і недоліки. Одній з сильних сторін підходу на базі гнучкого комутатора в даний час є його поширеність: в світі існує множина мереж, що пішли по цьому шляху розвитку, вже накопичений великий дослідний матеріал щодо впровадження архітектури Softswitch. Проте в рішенні на базі гнучкого комутатора є і недоліки. Різноманіття представленого в даному сегменті ринку устаткування породжує проблему його сумісності.

Деякі виробники устаткування надають фірмові системи управління мережею, які не завжди коректно і повноцінно працюють з устаткуванням сторонніх постачальників при його інтеграції в мережу оператора, оскільки є відмінності не тільки в реалізації, але і у функціональності багатьох систем.

Підхід на базі підсистеми IMS вигідно відрізняється наявністю стандартів, які надають можливість мати подібні, і тому здатні ефективно взаємодіяти, мережі. При цьому частково згладжуються проблеми сумісності устаткування, оскільки взаємодія функціональних модулів регулюється стандартами.

В принципі обидва підходи, по суті, мають одну і ту ж рівневу структуру. Як у одному, так і в іншому випадку необхідний єдиний мультисервісний абонентський доступ і єдиний IP-транспорт, акцент робиться на послуги для абонента, тому оператор при виборі стратегії побудови NGN повинен виходити, перш за все, з планованого набору послуг.

Резюмуючи вищенаведене зробимо наступні висновки.

NGN характеризується, з одного боку, як практична реалізація концепції Глобальної інформаційної інфраструктури (GII), яка у свою чергу є основою Глобального інформаційного суспільства (GIS) – суспільства XXI століття. З іншого боку, NGN повинна узаконити ті зміни в телекомунікаційних мережах, які сталися або почали здійснюватися останнім часом.

Головним принципом NGN є конвергенція всіх сфер в єдину інформаційну мережу із сприятливими можливостями для передачі мультимедійної інформації. NGN передбачає величезний набір послуг, що надаються користувачам. Кожен користувач повинен буде володіти персоніфікованим номером незалежно від використовуваних технологій доступу в будь-якому зручному для нього місці і у будь-який час. Він повинен мати можливість з'єднатися з визначеним іншим номером або кінцевим устаткуванням, або додатком (у тому числі для управління інформацією), користуватися мультимедійними додатками в реальному часі з дотриманням гарантованої якості обслуговування «з кінця в кінець». Користувачеві має бути надана необмежена мобільність без переривання сеансів в переміщенні і переході від однієї технології доступу до іншої. Проголошений в NGN набір послуг вельми складний з точки зору технічного і програмного забезпечення. Постулюється, що протоколи IP будуть основними в єдиній конвергованій мережі, використовуваними для надання служб NGN кінцевим користувачам, а також для підтримки традиційних служб. Передбачається переважання пакетного режиму відомих і вже діючих в даний час протоколів, в тому числі:

- для підтримки технології VoIP буде використовуватися стек H.323;
- для встановлення, модифікації викликів і завершення мультимедійних сесій протокол SIP;
- для встановлення віртуальних маршрутів за мітками - MPLS;
- для забезпечення класів гарантованого обслуговування RSVP-TE і CR-LDP.

Передбачається, що в NGN застосовуватиметься відкрите програмування. Спрощено це означає, що програмне забезпечення устаткування не буде «ноу-хау» фірм виробників, а виконуватиметься на традиційних загальновідомих мовах або ж будуть реалізовані програми-транслятори з відомих мов, що зменшить залежність операторів від постачальників устаткування.

Контрольні запитання

1. Назвіть рівні, якими може бути представлена архітектура мережі NGN.
2. Назвіть основні технології, які використовуються на рівні доступу.
3. Визначить переваги та недоліки комутації каналів.
4. Визначить переваги та недоліки комутації пакетів.
5. Назвіть основні технології, які використовуються на транспортному рівні мережі NGN.
6. На якому рівні згідно моделі взаємодії відкритих систем OSI функціонують волоконно-оптичні системи?
7. Які транспортні технології використовуються на канальному рівні згідно моделі взаємодії відкритих систем OSI?
8. На якому рівні згідно ієрархічної моделі NGN виконується функція обробка всіх видів сигналізації?
9. Який рівень згідно ієрархічної моделі NGN дозволяє реалізувати специфіку послуг?
10. Проведіть порівняльну характеристику функцій управління мережею на транспортному рівні і на рівні послуг для базової еталонної моделі NGN за концепцією ITU-T.

Розділ 3. Базові протоколи NGN. Стек протоколів TCP/IP

3.1. Визначення стека TCP/IP

Transmission Control Protocol/Internet Protocol (TCP/IP) – це промисловий стандарт стека протоколів, розроблений для глобальних мереж.

Стандарти TCP/IP розробляються групою Internet Engineering Task Force (IETF) і опубліковані в серії документів, названих Request for Comment (RFC).

Протоколи, що взаємодіють між собою, об'єднуються в стеки. Черговість виконання протоколів стека визначається операційною системою. На пристрої-відправнику протоколи стека виконуються зверху вниз, тобто від протоколів верхніх рівнів до протоколів нижніх рівнів. На пристрої (комп'ютері) - одержувачі протоколи стека виконуються від низу до верху.

3.2 Структура стека TCP/IP. Коротка характеристика протоколів

Оскільки стік TCP/IP був розроблений до появи моделі взаємодії відкритих систем ISO/OSI, то, хоча він також має багаторівневу структуру, відповідність рівнів стека TCP/IP рівням моделі OSI має досить умовний характер (рис.3.1).

<table>
<tr><th>Модель OSI</th><th></th><th>Модель TCP/IP</th></tr>
<tr><td>Прикладна</td><td rowspan="3"></td><td rowspan="3">Прикладна</td></tr>
<tr><td>Представницька</td></tr>
<tr><td>Сеансова</td></tr>
<tr><td>Транспортна</td><td></td><td>Транспортна</td></tr>
<tr><td>Мережева</td><td></td><td>Міжмережева</td></tr>
<tr><td>Канальна</td><td rowspan="2"></td><td rowspan="2">Інтерфейсна</td></tr>
<tr><td>Фізична</td></tr>
</table>

Рис. 3.1. Відповідність еталонних моделей OSI і TCP/IP

Структура протоколів TCP/IP приведена на рисунку 3.2. Протоколи TCP/IP розподіляються між чотирма рівнями.

Кожен рівень несе власне функціональне навантаження.

1. Канальний рівень (link layer) фактично об'єднує фізичний і канальний рівень моделі OSI. Ще його називають рівнем мережного інтерфейсу. Зазвичай включає драйвер пристрою в операційній системі і відповідну мережну

інтерфейсну плату в комп'ютері. Разом вони забезпечують апаратну підтримку фізичного з'єднання з мережею (з кабелем або з іншим використовуваним середовищем передачі). На фізичному рівні моделі ISO/OSI забезпечується передача бітових потоків по фізичному носієві. Цей рівень в протоколах TCP/IP не регламентується, але підтримує всі популярні стандарти фізичного і канального рівня: для локальних мереж це Ethernet, Token Ring, FDDI, Fast Ethernet; для глобальних мереж - протоколи з'єднань "точка-точка" SLIP і PPP, протоколи територіальних мереж з комутацією пакетів X.25, Frame relay.

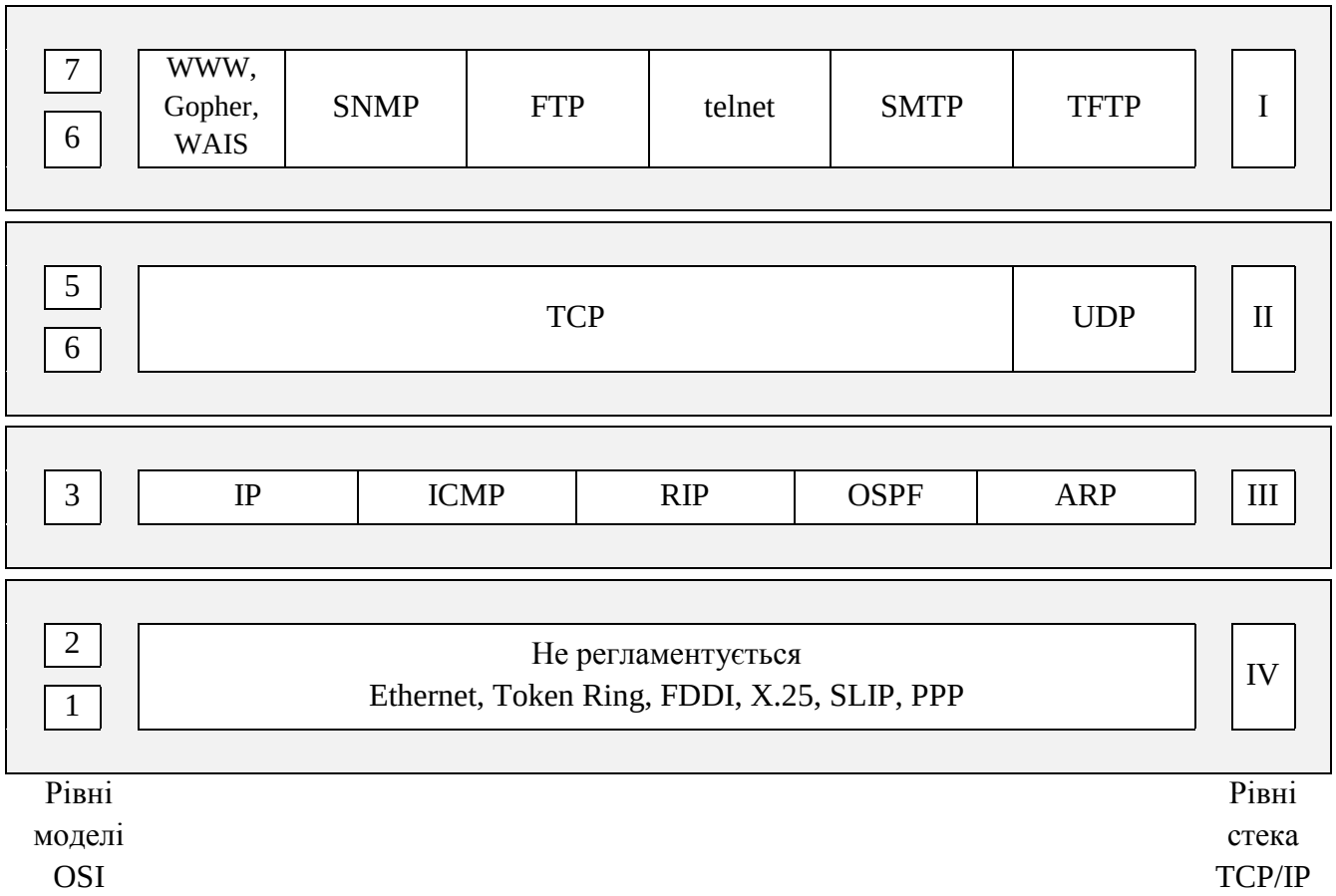


Рис. 3.2. Стек TCP/IP

2. Мережний рівень (network layer), інколи званий рівнем міжмережної взаємодії, відповідає за передачу пакетів по мережі. Маршрутизація пакетів здійснюється саме на цьому рівні. IP (Internet Protocol - протокол Internet), ICMP (Internet Control Message Protocol - протокол управління повідомленнями Internet) і IGMP (Internet Group Management Protocol - протокол управління групами Internet) забезпечують мережний рівень в сімействі протоколів TCP/IP. До рівня міжмережної взаємодії відносяться і всі протоколи, пов'язані із складанням і модифікацією таблиць

маршрутизації, такі як протоколи збору маршрутної інформації RIP (Routing Internet Protocol) і OSPF (Open Shortest Path First)

3. Транспортний рівень (transport layer) відповідає за передачу потоку даних між двома комп'ютерами і забезпечує роботу прикладного рівня, який знаходиться вище. У сімействі протоколів TCP/IP існує два транспортні протоколи: TCP (Transmission Control Protocol) і UDP (User Datagram Protocol). TCP здійснює надійну передачу даних між двома комп'ютерами. Він забезпечує ділення даних, що передаються від одного додатка до іншого, на пакети відповідного для мережного рівня розміру, підтвердження прийнятих пакетів, установлення тайм-аутів, протягом яких повинне прийти підтвердження на пакет, і так далі. Оскільки надійність передачі даних гарантується на транспортному рівні, на прикладному рівні ці деталі ігноруються. UDP надає простіший сервіс для прикладного рівня. Він просто посилає пакети, які називаються дейтаграмами (datagram) від одного комп'ютера до іншого. При цьому немає жодної гарантії, що дейтаграма дійде до пункту призначення. За надійність передачі даних, при використанні дейтаграмм, відповідає прикладний рівень. Для кожного транспортного протоколу існують різні додатки, які їх використовують.
4. Прикладний рівень (application layer) визначає деталі кожного конкретного додатку. Існує декілька поширених застосувань TCP/IP, які присутні практично в кожній реалізації:
   - Telnet – віддалений термінал;
   - FTP, File Transfer Protocol – протокол передачі файлів;
   - SMTP, Simple Mail Transfer Protocol – простий протокол передачі електронної пошти;
   - SNMP, Simple Network Management Protocol – простий протокол управління мережею.

Коли додаток посилає дані з використанням TCP, дані опускаються вниз по стеку протоколів, проходячи через кожен рівень, до тих пір, поки вони не будуть відправлені у вигляді потоку бітів по мережі. Кожен рівень додає свою інформацію до даних щляхом пристикування заголовків (а інколи завершувачів, трейлерів). На рисунку 3.3 показаний цей процес. Блок даних, який TCP посилає в IP, називається TCP сегментом. Блок даних, який IP посилає в мережний інтерфейс, називається IP-дейтаграмою. Потік бітів, який передається по Ethernet, називається фреймом (frame) або кадром. Наприклад, пакети TCP інкапсулюються в IP-дейтаграми, IP-дейтаграми інкапсулюються в кадри Ethernet.

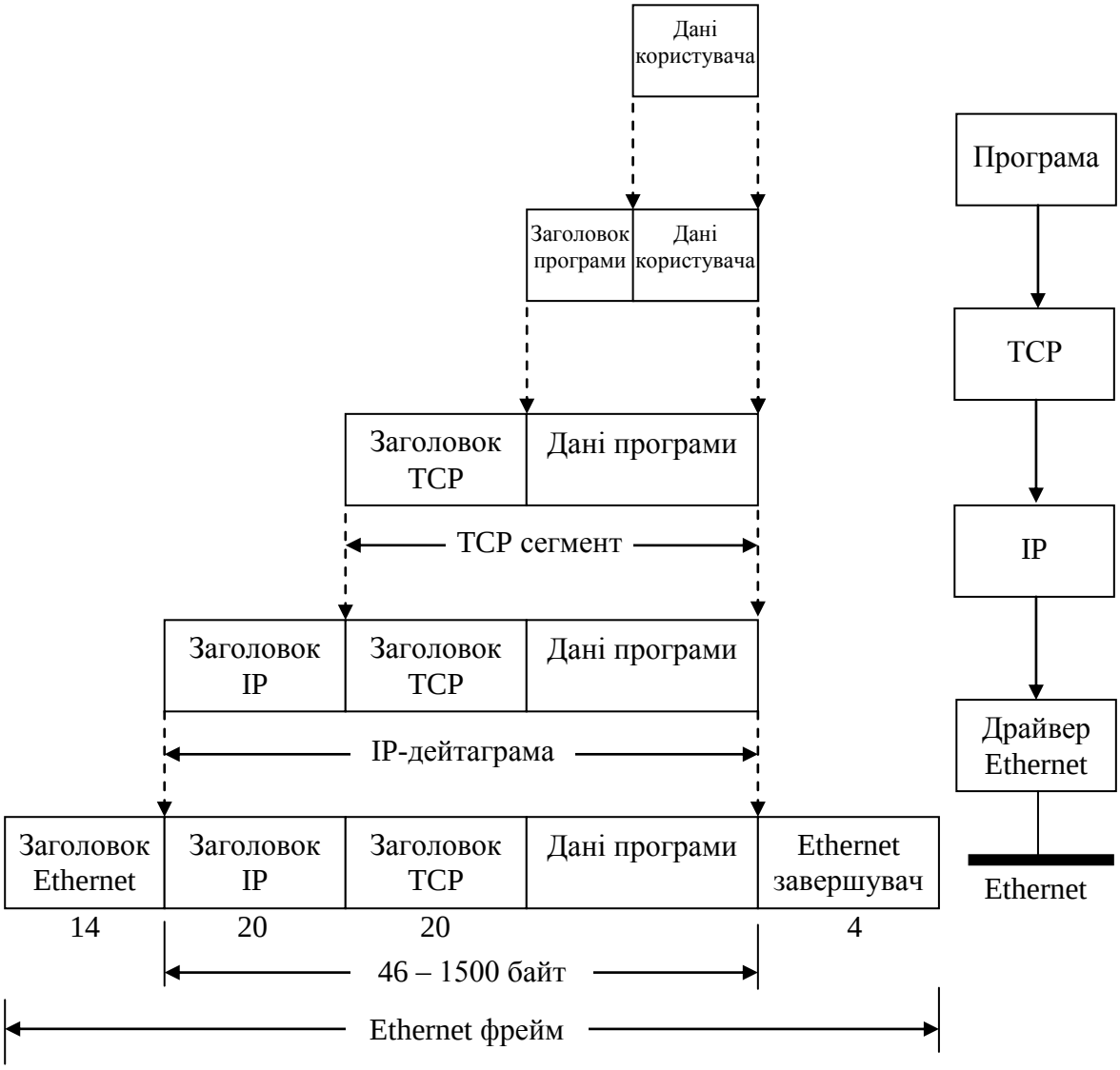


Рис. 3.3. Інкапсуляція даних по мірі того як вони проходять по стеку протоколів.

Розглянемо основні принципи функціонування мережевого протоколу IP і транспортного TCP.

3.3. Протокол IP

Протокол IP є протоколом мережного (3-го) рівня, який містить інформацію об адресації і управляючу інформацію для маршрутизації пакетів. Протокол IP описаний в RFC 791 і є основним протоколом мережного рівня в наборі протоколів Internet. Разом з протоколом управління передачею (TCP) протокол IP утворює основу протоколів Internet. Протокол IP має дві основні функції: забезпечення передачі дейтаграм по об'єднаній мережі методом негарантованої доставки без підтвердження з'єднання і забезпечення

фрагментації і повторної збірки дейтаграм для підтримки каналів передачі даних з різними розмірами максимального передаваного модуля даних (MTU).

IP – ненадійний протокол, що надає сервіс доставки дейтаграм без з'єднання. Це означає, що не існує гарантії того, що IP дейтаграма успішно досягне пункту призначення. Проте IP надає певний сервіс обробки деяких подій. Коли що-небудь йде не так як хотілося б, як наприклад, тимчасове переповнювання буфера маршрутизатора, IP застосовує простий алгоритм обробки помилок: він відкидає дейтаграму і прагне послати ICMP повідомлення відправнику. Будь-яка необхідна надійність має бути забезпечена верхніми рівнями (наприклад, TCP).

Термін без з'єднання (connectionless) означає, що IP не містить жодної інформації про просування дейтаграм. Кожна дейтаграма обробляється незалежно від інших. Це також означає, що може бути доставлена зіпсована дейтаграма. Якщо джерело відправляє дві послідовні дейтаграммы (перша A, потім B) в один і той же пункт призначення, кожна з них маршрутизується незалежно і може пройти за різними маршрутами, тобто дейтаграма B може прибути раніше чим A.

3.3.1. Формат пакету IP

IP-пакет складається із заголовка і поля даних. Заголовок зазвичай має довжину 20 байт. Розглянемо його структуру (рис. 3.4).

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Version				IHL				DSCP						ECN		Total Length															
4	32	Identification																Flags			Fragment Offset											
8	64	Time To Live								Protocol								Header Checksum															
12	96	Source IP Address																															
16	128	Destination IP Address																															
20	160	Options (if IHL > 5)																															

Рис.3.4. Формат заголовку пакета IPv4

Старший значущий біт має номер 0 (зліва), а молодший значущий біт з 32-х біт має номер 31 і показаний справа. Чотири байти з 32-бітового значення передаються в наступному порядку: спочатку біти 0 - 7, потім біти 8 - 15, потім 16 - 23 і, нарешті, 24 - 31. Такий порядок руху байтів обов'язковий для всіх двійкових цілих чисел в TCP заголовках при їх передачі по мережі.

Поле Версія (Version) (довжина 4 біта) вказує версію протоколу IP. Нагадаємо, що зараз ми розглядаємо протокол IP версії 4 (IPv4).

Поле Довжина заголовка (IHL) (довжина 4 біта) вказує довжину заголовка в 32-бітових словах. Зазвичай заголовок має довжину 20 байт (що дорівнює п'яти 32-бітових словам), проте можливе включення в заголовок додаткової інформації, розміщеної в полі Опції. Максимальна довжина заголовка - 60 байт (що дорівнює п'ятнадцяти 32-бітових словам)

Диференційоване обслуговування Кодової точки (Differentiated Services Code Point (DSCP)). Спочатку поле визначається як Тип обслуговування, в цьому полі тепер визначається для диференційованого обслуговування (DiffServ). З'являються нові технології, які вимагають прослуховування даних в реальному часі і, отже, використовувати поле DSCP. Прикладом може служити передача голосу по IP (VoIP), яка використовується для інтерактивного обміну мовними даними.

Поле Тип обслуговування (Type of Service, ToS) (довжина 8 біт) складається з декількох підполів (рис.3.5). Спочатку йде підполе пріоритету (Precedence) пакету (довжина 3 біта). Пріоритет може мати значення від найнижчого - 0 (звичайний пакет) до найвищого - 7 (пакет управляючої інформації). Важливіші пакети обробляються в першу чергу.

0	1	2	3	4	5	6	7
Precedence			D	T	R	C	

Рис. 3.5. Поле *Тип обслуговування* заголовку IP

Далі слідують чотири біта, що задають тип обслуговування. З цих чотири біт лише один може бути виставлений в 1. Вони мають таку сутність: мала затримка (Low Delay, D), висока пропускна спроможність (High Throughput, T), висока надійність (High Reliability, R), низька вартість (Low Cost, C). Останній біт підполя був доданий вже після появи RFC 791 і на даний час не використовується.

У таблиці 3.1 показані рекомендовані значення поля ToS для різних застосувань.

Діалогові додатки, Telnet і Rlogin, вимагають звести до мінімуму затримку, оскільки вони використовуються людиною в інтерактивному режимі і здійснюють передачу невеликого обсягу даних. Передача файлів з використанням FTP, з іншого боку, вимагає максимальної пропускної спроможності. Максимальна надійність необхідна для мережного управління (SNMP) і для протоколів маршрутизації.

Поле повідомлення про перевантаження (Explicit Congestion Notification (ECN)). Це поле дозволяє передавати повідомлення про перевантаження мережі без відкидання пакетів. ECN є додатковою функцією, яка використовується

тільки, коли обидві кінцеві точки підтримують його і готові його використовувати. Він ефективний тільки тоді, коли підтримується мережею.

Поле Загальна довжина (Total Length) (довжина 16 біт) описує загальний розмір пакету в байтах з врахуванням заголовка і поля даних. Максимальна довжина пакету обмежена розрядністю цього поля і складає 65535 байт, проте зазвичай настільки великі пакети не використовуються. Завдяки цьому полю і полю довжини заголовка, ми знаємо, з якого місця починаються дані в IP дейтаграмі і їх довжину.

Таблиця 3.1

Рекомендовані значення поля ToS

Додаток	**Мінімізація затримки**	**Максимізація продуктивності**	**Максимізація надійності**	**Мінімізація вартості**
Telnet/Rlogin	1	0	0	0
FTP				
управління	1	0	0	0
дані	0	1	0	0
SMTP				
фаза команд	1	0	0	0
фаза даних	0	1	0	0
DNS				
UDP запит	1	0	0	0
TCP запит	0	0	0	0
SNMP	0	0	1	0
NNTP	0	0	0	1

Поле Ідентифікатор пакету (Identification) (довжина 16 біт) визначає кожен посланий вузлом пакет IP і збільшується на 1 при відправці кожного пакету. Виключенням з правил є фрагментовані пакети IP, в яких значення поля ідентифікатора пакету однаково для всіх відправлених фрагментів. При фрагментації використовуються також поля Прапори і Зсув фрагмента.

Поле Flags (довжина 3 біта) містить ознаки, пов'язані з фрагментацією, а саме, встановлений біт DF забороняє маршрутизатору фрагментувати даний пакет, а біт MF (More Fragments) говорить про те, що даний пакет є проміжним фрагментом і далі ще є фрагменти. Перший біт зарезервований.

Поле Зсув фрагмента (Fragment Offset) (довжина 13 біт) задає зсув в байтах поля даних цього пакету від початку поля даних вихідного фрагментованого пакету. Зсув має бути кратним 8 байтам.

Поле Час життя (Time to Live, TTL) (довжина 8 біт) вказує граничний термін, протягом якого пакет може переміщатися по мережі. Значення цього поля встановлюється відправником (як правило 32 або 64) і зменшується на 1, кожний раз, коли пакет IP проходить через маршрутизатор. Коли значення цього

поля досягає 0, маршрутизатор відкидає пакет і посилає відправникові пакет ICMP, повідомляючи його про закінчення часу життя. Основним призначенням цього пакету є запобігання зацикленню пакету між маршрутизаторами. Якщо одержувач прийняв не всі фрагменти пакету IP, а поле Час життя дорівнює нулю, то одержувач направляє відправникові пакет ICMP, що повідомляє про закінчення Часу життя вже в процесі чекання початку збірки пакету.

Поле Протокол верхнього рівня вказує, якому протоколу верхнього рівня належить інформація, що розміщена в полі даних пакету. Значення ідентифікаторів для різних протоколів наводяться в RFC. Наприклад, протоколу TCP відповідає значення 6, протоколу UDP -17, протоколу зовнішнього шлюзу EGP - 8, при інкапсуляції IP в IP - 4, протоколу міжмережних управляючих повідомлень ICMP -1, протоколу маршрутизації OSPF -89.

Поле Контрольна сума (Header Checksum) (довжина 2 байти) розраховується лише по заголовку (дані не враховуються). Оскільки деякі поля заголовка міняють своє значення в процесі передачі пакету по мережі, контрольна сума перевіряється і повторно розраховується при кожній обробці заголовка пакету IP. При обчисленні контрольної суми значення самого поля Контрольна сума виставляється в нуль.

Поля IP-адрес джерела (Source IP Address) і IP-адрес призначення (Destination IP Address) (довжина по 32 біта) містять адреси відправника і одержувача відповідно.

Поле Опції (Option) є необов'язковим і використовується зазвичай при відладці.

3.3.2. IP-маршрутизація

Розглянемо загальні принципи IP-маршрутизації. Відповідно до загальної схеми, рівень IP може отримувати блок даних від власних рівнів TCP, UDP, ICMP і IGMP (це дейтаграми, що формуються на цьому же пристрої). В цьому випадку дейтаграма формується і передається для подальшої обробки нижньому рівню (мережному інтерфейсу) і потім передається в канал. В іншому разі дейтаграми можуть бути прийняті з якого-небудь мережного інтерфейсу.

Якщо мережний вузол є джерелом інформації і, якщо пункт призначення безпосередньо підключений до хосту (наприклад, канал "точка-точка") або хост включений між декількома мережами (Ethernet або Token ring), IP-дейтаграма прямує безпосередньо в пункт призначення, інакше хост посилає дейтаграму на маршрутизатор за умовчанням, тим самим надаючи маршрутизатору право вирішувати як доставити дейтаграму в пункт призначення (основна різниця між хостом і маршрутизатором полягає в тому, що хост ніколи не перенаправляє

дейтаграми з одного свого інтерфейсу на іншій, тоді як маршрутизатор перенаправляє).

Якщо дейтаграма прийнята з мережного інтерфейсу, то:

1) IP перевіряє, чи не належить йому вказаний IP-адрес призначення або чи не є цій IP-адрес широкомовним. Якщо це так, то дейтаграма доставляється в модуль протоколу, вказаний в полі протоколу IP-заголовка.

2) Якщо дейтаграма не призначається для цього IP-рівня і, якщо IP-рівень не був сконфігурований як маршрутизатор, дейтаграма знищується.

3) Якщо IP-рівень сконфігурований для того, щоб працювати як маршрутизатор, пакет перенаправляється.

IP-рівень, сконфігурований як маршрутизатор, має в пам'яті таблицю маршрутизації, яку він переглядає кожного разу при здобутті дейтаграми, яку необхідно перенаправити.

Кожен пункт таблиці маршрутизації містить наступну інформацію:

- IP-адрес призначення. Це може бути як повний адрес хоста (host address) або адрес мережі (network address), що вказується в полі прапорів. Адрес хоста має ненульове значення ідентифікатора хоста і вказує на один конкретний хост, тоді як адрес мережі має ідентифікатор хоста, встановлений в 0, і вказує на всі хости, включені в певну мережу (Ethernet, Token ring).
- IP-адрес маршрутизатора наступної пересилки (next-hop router), або, інакше кажучи, IP-адрес безпосередньо підключеної мережі. Маршрутизатор наступної пересилки належить одній з безпосередньо підключених мереж, в яку ми можемо відправити дейтаграми для їх доставки. Маршрутизатор наступної пересилки це не кінцевий пункт призначення, проте він приймає дейтаграми, які ми посилаємо, і перенаправляє їх у напрямі кінцевого пункту.
- Прапори. Один прапор вказує, чи є IP-адрес пункту призначення, адресом мережі або адресом хоста. Інший прапор вказує на те, чи є маршрутизатор наступної пересилки дійсно маршрутизатором або це безпосередньо підключений інтерфейс.
- Вказівка на те, на який мережний інтерфейс мають бути передані дейтаграми для передачі.

IP-маршрутизація здійснюється за принципом пересилка за пересилкою. Як ми можемо побачити з таблиці маршрутизації, IP не знає повний маршрут до пункту призначення (за винятком тих пунктів призначення, які безпосередньо підключені до посилаючого хосту). Все що може надати IP-маршрутизація - це IP-адрес маршрутизатора наступної пересилки, на який посилається дейтаграмма. При цьому робиться припущення, що маршрутизатор наступної пересилки ближче до пункту призначення, ніж посилаючий хост.

IP-маршрутизація здійснює наступні дії:

1. Здійснюється пошук в таблиці маршрутизації, при цьому шукається пункт, який співпадає з повним адресом пункту призначення (повинні збігтися ідентифікатор мережі і ідентифікатор хоста). Якщо пункт знайдений в таблиці маршрутизації, пакет посилається на вказаний маршрутизатор наступної пересилки або на безпосередньо підключений інтерфейс (залежно від поля прапорів). Як правило, так визначаються канали точка-точка, при цьому інший кінець такого каналу, як правило, є повним IP-адресом віддаленого хоста.
2. Здійснюється пошук в таблиці маршрутизації пункту, який співпадає, як мінімум, з ідентифікатором мережі призначення. Якщо пункт знайдений, пакет посилається на вказаний маршрутизатор наступної пересилки або на безпосередньо підключений інтерфейс (залежно від поля прапорів). Маршрутизація по відношенню до всіх хостів, що знаходяться в мережі призначення, здійснюється з використанням цього єдиного пункту таблиці маршрутизації (наприклад, всі хости локальної мережі Ethernet). Ця перевірка збігу ідентифікатора мережі здійснюється з використанням можливої маски підмережі.
3. У таблиці маршрутизації шукається пункт, помічений "за умовчанням" (default). Якщо пункт знайдений, пакет відсилається на вказаний маршрутизатор за умовчанням.

Якщо жоден з кроків не дав позитивного результату, дейтаграма вважається недоставленою. Якщо недоставлену дейтаграму згенерувано даним хостом, то зазвичай повертається помилка "хост недоступний" (host unreachable) або "мережа недоступна" (network unreachable). Цей код помилки повертається застосуванню, яке створило дейтаграмму.

На початку завжди здійснюється порівняння на співпадання повного адресу хоста, після чого здійснюється порівняння ідентифікатора мережі. Лише в тому випадку, якщо результат обох порівнянь негативний, використовується маршрут за умовчанням. Маршрути за умовчанням і повідомлення ICMP про перенаправлення, що відправляються на маршрутизатор наступної пересилки (якщо для дейтаграми вибраний невірний напрям за умовчанням), є важливими характеристиками IP-маршрутизації.

Ще одна фундаментальна характеристика IP-маршрутизації полягає в можливості вказати маршрут до мережі, замість того, щоб вказувати маршрут до кожного окремо взятого хосту. Саме тому хости, що включені в Internet, мають в своїх таблицях маршрутизації тисячі пунктів, замість того аби містити в них більше за мільйон пунктів.

3.3.3. Схема адресації протоколу IPv4

У мережі IP всі пристрої мають унікальний адрес (IP-адрес). IP-адрес характеризує не само пристрій, а з'єднання пристрою з мережею (наприклад, пристрій з двома мережними інтерфейсами матиме як мінімум два IP- адреси). Схема адресації протоколу IPv4 описана в документах RFC 990, RFC 997.

IP-адрес має довжину 32 біта. Для зручності прийнято записувати IP-адрес у вигляді двійково-десяткового числа: кожен байт (октет) записується у вигляді десяткового числа в діапазоні від 0 до 255; октети розділені крапками (наприклад, 192.168.0.1). Така форма запису носить назву десятково-точкової нотації.

Класи адрес. IP-адреса розділяються на 5 класів: A, B, C, D, E. Адреси класів A, B і C діляться на дві логічні частини: номер мережі і номер вузла (рис. 3.6).

В адресі класу A старший біт встановлений в 0. Довжина мережного префікса - 8 біт. Для номера вузла виділяється 24 біта.

В адресі класу B два старших біта встановлені в 1 і 0 відповідно. Довжина мережного префікса - 16 біт. Поле номера вузла теж має довжину 16 біт.

В адресі класу C три старших біта встановлені в 1, 1 і 0 відповідно. Префікс мережі має довжину 24 біта, номер вузла - 8 біт.

Два класи, що залишилися, мають іншу структуру адресу.

В адресі класу D чотири старших біта встановлені в 1, 1, 1 і 0 відповідно. Адреси цього класу використовуються для підтримки групового мовлення (Multicasting). При груповому мовленні пакет передається декільком вузлам за схемою «один-до-багатьох». Адрес класу D є ідентифікатором такої групи. Вузли самі ідентифікують себе, визначаючи, до якої групи вони відносяться. Вузли, що належать одній групі, можуть бути розподілені по різних мережах довільним чином.

В адресі класу E чотири старших біта встановлені в 1, 1, 1 і 1 відповідно. Клас E зарезервований для експериментального використання.

Класи мереж	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Клас A	0	№ мережі							№ вузла																							
Клас B	1	0	№ мережі														№ вузла															
Клас C	1	1	0	№ мережі																					№ вузла							
Клас D	1	1	1	0	Адреса групи multicast																											
Клас E	1	1	1	1	0	Зарезервовано																										

Рис. 3.6. Класи мереж IPv4

Розглянемо поняття "маска підмережі (мережі)". Маскою підмережі або маскою мережі називається бітова маска, що визначає, яка частина IP-адреса вузла мережі відноситься до адресу мережі, а яка - до адресу самого вузла в цій мережі.

Поля номерів мережі і підмережі утворюють розширений мережний префікс. Для виділення розширеного мережного префікса використовується маска підмережі (Subnet Mask) - 32-розрядне двійкове число (по довжині IP-адреса), в розрядах розширеного префікса що містить одиницю, а в останніх розрядах - нуль, інакше кажучи маска містить біти, встановлені в одиницю для ідентифікатора мережі і ідентифікатора підмережі, і біти, встановлені в 0 для ідентифікатора хоста.

Розширений мережний префікс виходить побітовим порозрядним множенням (логічне "I") IP-адреса і маски підмережі. При такій побудові вочевидь, що число підмереж є мірою двійки – 2n, де n - довжина поля номера підмережі. Таким чином, характеристики IP-адреса повністю задаються власне IP-адресом і маскою підмережі.

Для спрощення запису застосовують наступну нотацію (так звана CIDR - нотація):

IP-адрес/довжина розширеного мережного префікса.

Число після слеша означає кількість одиничних розрядів, що містяться в масці підмережі.

Наприклад, адрес 192.168.0.1 з маскою 255.255.255.0 в даній нотації виглядатиме як /24 (тобто кількість одиниць в масці дорівнює 24).

Для стандартних класів мереж можна записати наступні значення масок підмереж (у десятково-точковій нотації):

- 255.0.0.0 - маска для мережі класу A; довжина розширеного мережного префікса - 8;
- 255.255.0.0 - маска для мережі класу B; довжина розширеного мережного префікса - 16;
- 255.255.255.0 - маска для мережі класу C; довжина розширеного мережного префікса - 24.

3.4. Протокол TCP

Протокол управління передачею (Transmission Control Protocol, TCP) є протоколом транспортного рівня, який має засоби управління потоком і корекції

помилок. Він орієнтований на встановлення з'єднання, тому клієнт зобов'язаний встановити з'єднання з сервером до початку передачі даних TCP в будь-якому з напрямів (RFC 793).

TCP забезпечує свою надійність завдяки наступному:

- Дані від додатку розбиваються на блоки певного розміру, які будуть відправлені. Це повністю відрізняється від UDP, в якому кожен запис, який здійснює додаток, генерує IP-дейтаграмму цього розміру. Блок інформації, який передається від TCP в IP, називається сегментом (segment).
- Коли TCP посилає сегмент, він встановлює таймер, чекаючи, що з віддаленого кінця прийде підтвердження на цей сегмент. Якщо підтвердження не отримане після закінчення часу, сегмент передається повторно.
- Коли TCP приймає дані від віддаленої сторони з'єднання, він відправляє підтвердження. Це підтвердження не вирушає негайно, а зазвичай затримується на долі секунди
- TCP здійснює розрахунок контрольної суми для свого заголовка і даних. Це контрольна сума, що розраховується на кінцях з'єднання, метою якої є виявити будь-яку зміну даних в процесі передачі. Якщо сегмент прибуває з невірною контрольною сумою, TCP відкидає його і підтвердження не генерується. При цьому, очікується, що відправник відпрацює тайм-аут і здійснить повторну передачу.
- Оскільки TCP сегменти передаються у вигляді IP - дейтаграм, а IP - дейтаграми можуть прибувати хаотично, також хаотично (без дотримання черги) можуть прибувати і TCP сегменти. Після отримання даних TCP може за необхідністю змінити їх послідовність, в результаті чого додаток отримує дані в правильному порядку.
- Оскільки IP - дейтаграма може бути продубльована, приймаючий TCP повинен відкидати продубльовані дані.
- TCP здійснює контроль потоку даних. Кожна сторона TCP з'єднання має буфер певного розміру. TCP на приймаючій стороні дозволяє віддаленій стороні посилати дані лише в тому випадку, якщо одержувач може помістити їх в буфер. Це запобігає від переповнювання буферів хостів з невисокою продуктивністю швидкими хостами.

3.4.1. Формат пакету TCP

Структуру заголовка сегменту TCP наведено на рис. 3.7.

Поля Порт джерела (Source Port) (довжина 16 біт) і Порт одержувача (Destination Port) (довжина 16 біт) ідентифікують процес, що використовує протокол TCP. Ці два значення разом з IP-адресом джерела і призначення в IP-

заголовку унікально ідентифікують кожне з'єднання. Комбінація IP-адреса і номера порту інколи називається сокетом (socket) .

Поля Порядковий номер (Sequence Number) (довжина 32 біта) і Номер підтвердження (Acknowledgement Number) (довжина 32 біта) нумерують кожен відправлений або отриманий байт даних. Ці поля реалізуються як цілі числа без знаку, які скидаються, коли досягають максимального значення. Кожна сторона веде власну порядкову нумерацію.

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	Source port																Destination port															
4	32	Sequence number																															
8	64	Acknowledgment number (if ACK set)																															
12	96	Data offset				Reserved			NS	CWR	ECE	URG	ACK	PSH	RST	SYN	FIN	Window Size															
16	128	Checksum																Urgent pointer (if URG set)															
20	160	Options (if *data offset* > 5. Padded at the end with "0" bytes if necessary.)																															

Рис. 3.7. Формат заголовка пакету TCP

Поле Довжина заголовка (Offset) (довжина 4 біта) містить розмір TCP-заголовка в 32-бітових словах. Ця інформація необхідна, оскільки поле Параметри (Option) може бути змінної довжини. Можна сказати, що це поле задає зсув від початку сегменту до початку даних в 32-бітових словах.

Слідом іде зарезервоване поле (Resrvd) завдовжки 6 біт.

Поле Прапори (довжина 9 біт), що містить дев’ять однобітових прапорів.

Прапор NS (1 біт) – ECN-nonce concealment protection приховування одноразовий захисту

Прапор CWR (1 біт) - вікна зниження перевантаження (Congestion Window Reduced (CWR)). Прапор встановлюється отправляющим хостом, щоб вказати, що він отримав сегмент TCP з прапором ECE встановленим в механізмі управління перевантаженням.

Прапор ECE (1 біт) - ECN-Echo індикатор

Якщо прапор SYN встановлено (1), то TCP дорівнює ECN можливостям.

Якщо прапор SYN вільний (0), то пакет з перевантаженнями перевірений прапором в комплекті заголовка IP отримано при нормальній передачі.

Прапор Покажчик терміновості (Urgent Pointer, URG) встановлюється в одиницю в випадку використання поля Покажчик на термінові дані.

Прапор Підтвердження (Acknowledgment, ACK) встановлюється в одиницю в разі, якщо поле Номер підтвердження (Acknowledgement Number) містить дані. Інакше це поле ігнорується.

Прапор Виштовхування (Push, PSH) означає, що приймаючий стек TCP повинен негайно інформувати додаток про дані, що поступили, а не чекати, поки буфер заповниться. Деякі сучасні реалізацій TCP просто ігнорують прапор PSH під час прийому пакетів.

Прапор Скидання (Reset, RST) використовується для відміни з'єднання із-за помилки додатку, відмови від невірного сегменту, спроби створити з'єднання за відсутності сервісу, що вимагався.

Прапор Синхронізація (Synchronize, SYN) встановлюється при ініціації з'єднання і синхронізації порядкового номера.

Прапор Завершення (Finished, FIN) використовується для розриву з'єднання. Він вказує, що відправник закінчив передачу даних.

Управління потоком в протоколі TCP здійснюється за допомогою ковзаючого вікна змінного розміру. Поле Розмір вікна (Window) (довжина 16 біт) містить кількість байт, яке може бути послане після байта, отримання якого вже підтверджене. Якщо значення цього поля дорівнює нулю, це означає, що всі байти, аж до байта з номером, який відповідає значенню поля Номер підтвердження, отримані, але одержувач відмовляється приймати подальші дані. Дозвіл на подальшу передачу може бути виданий відправкою сегменту з таким же значенням поля Номер підтвердження і ненульовим значенням поля Розмір вікна.

Поле Контрольна сума TCP (Checksum) (довжина 16 біт) містить контрольну суму пакету TCP, що обчислюється по всьому пакету TCP з доданим псевдозаголовком (рис. 3.9). Під час обчислення контрольної суми це поле виставляється в нуль, а поле даних вирівнюється за 32-байтною межею нульовими байтами.

<table>
<tr><td>Offsets</td><td>Octet</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>Octet</td><td>Bit</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td>0</td><td>0</td><td colspan="32">Source address</td></tr>
<tr><td>4</td><td>32</td><td colspan="32">Destination address</td></tr>
<tr><td>8</td><td>64</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td>0</td><td colspan="8">Protocol</td><td colspan="16">TCP length</td></tr>
<tr><td>12</td><td>96</td><td colspan="16">Source port</td><td colspan="16">Destination port</td></tr>
<tr><td>16</td><td>128</td><td colspan="32">Sequence number</td></tr>
<tr><td>20</td><td>160</td><td colspan="32">Acknowledgment number</td></tr>
<tr><td>24</td><td>192</td><td colspan="4">Data offset</td><td colspan="3">Reserved</td><td colspan="9">Flags</td><td colspan="16">Window</td></tr>
<tr><td>28</td><td>224</td><td colspan="16">Checksum</td><td colspan="16">Urgent pointer</td></tr>
<tr><td>32</td><td>256</td><td colspan="32">Options (optional)</td></tr>
<tr><td></td><td>288</td><td colspan="32">Data</td></tr>
</table>

Рис. 3.9. Структура пакету TCP при обчисленні контрольної суми

Псевдозаголовок формується виключно для роботи з контрольною сумою і має наступну структуру (рис.3.10).

Offsets	Octet	0								1								2								3							
Octet	Bit	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	0	IP-адрес джерела (Source address)																															
4	32	IP-адрес одержувача (Destination address)																															
8	64	0	0	0	0	0	0	0	0	Протокол (Protocol)								Длина TCP-сегмента (TCP length)															

Рис. 3.10. Структура псевдозаголовка пакету TCP

Спочатку йдуть поля IP-адрес джерела (довжина 32 біт) і IP-адрес одержувача (довжина 32 біт). Далі йде зарезервоване поле (довжина 8 біт), заповнене нулями.

Поле Протокол (довжина 8 біт) ідентифікує протокол із заголовка пакету IP. Для TCP це значення дорівнює 6 . Далі йде поле Довжина TCP (довжина 16 біт).

Поле Покажчик на термінові дані (довжина 16 біт) містить зсув в байтах від поточного порядкового номера байта до місця розташування термінових даних. Вмістом термінових даних займаються вищестоящі рівні.

Поле Параметри (Option) (довжина змінної, кратна 32 бітам) містить додаткові поля, що розширюють можливості стандартного заголовка. Це поле зарезервоване для майбутнього вживання і в заголовку може бути відсутнім.

Дані в TCP-сегменті можуть бути і відсутніми, характер і формат передаваної інформації задаються виключно прикладною програмою, теоретично максимальний розмір цього поля складає за відсутністю опцій 65495 байт. Максимальний розмір сегменту (MSS) це найбільша порція даних, яку TCP пошле на віддалений кінець, за умовчанням це 536 байт (в цьому випадку, при 20-байтному IP-заголовку і 20-байтному TCP-заголовку, розмір IP дейтаграми складатиме 576 байт).

У загальному випадку, чим більше MSS тим краще, до тих пір, поки не відбувається фрагментація. Великі розміри сегменту дозволяють послати більше даних в кожному сегменті, що зменшує відносну вартість IP і TCP заголовків. Коли TCP відправляє SYN сегмент, або коли локальний додаток хоче встановити з'єднання, або коли прийнятий запит на з'єднання від віддаленого вузла, може бути встановлене значення MSS рівне MTU вихідного інтерфейсу мінус розмір фіксованих TCP і IP заголовків. Для Ethernet MSS може досягати 1460 байт (дорівнює 1500-20-20). При використанні механізму інкапсуляції за IEEE 802.3 MSS може бути до 1452 байт (дорівнює 1492-20-20).

3.4.2. Встановлення сесії TCP

Поля Порядковий номер (Sequence Number) і Номер підтвердження (Acknowledgment Number) грають роль лічильника пакетів. При встановленні сесії використовується поле прапорів.

Встановлення зв'язку клієнт-сервер здійснюється в три етапи (триступінчате рукостискання - three way handshake) (рис. 3.11).

Нехай хост А створює з'єднання з хостом В.

1) Режим активного доступу (Active Open). Клієнт посилає повідомлення SYN, ISNa, тобто в передаваному повідомленні встановлений біт SYN (Synchronize Sequence Number), а в полі Порядковий номер (Sequence Number) – початкове 32-бітове значення ISNa (Initial Sequence Number - початковий порядковий номер хоста А для передачі).

2) Режим пасивного доступу (Passive Open). Сервер відгукується, посилаючи повідомлення SYN, ACK, ISNb (Initial Sequence Number хоста В), ACK (що дорівнює ISSa+1), тобто встановлені біти SYN і ACK; у полі Порядковий номер (Sequence Number) хостом В встановлюється початкове значення лічильника - ISNb; поле Номер підтвердження (Acknowledgment Number) містить значення ISNa, отримане в першому пакеті від хоста А і збільшене на одиницю.

3) Завершення рукостискання. Клієнт відправляє підтвердження отримання SYN-сегмента від сервера з ідентифікатором, рівним ISN сервера збільшений на одиницю: ACK, ISNa+1, ACK (ISNb+1). У цьому пакеті встановлений біт ACK, поле Порядковий номер (Sequence Number) містить ISNa+1, поле Номер підтвердження (Acknowledgment Number) містить значення ISNb+1. Посилкою цього пакету закінчується триступінчате рукостискання, і TCP- з'єднання вважається встановленим.

4) Тепер клієнт може посилати пакети з даними на сервер по тільки що створеному віртуальному TCP-каналу: ACK, ISSa+1, ACK(ISSb+1); DATA.

З розглянутої вище схеми створення TCP- з'єднання видно, що єдиними ідентифікаторами TCP-абонентів і TCP- з'єднання є два 32-бітові параметри: Порядковий номер (Sequence Number) і Номер підтвердження (Acknowledgment Number).

Приклад встановлення і розриву з'єднання – встановлення TCP-з'єднання [20]:

1. Запрошуюча сторона (яка, як правило, називається клієнт) відправляє SYN сегмент, вказуючи номер порту сервера, до якого клієнт хоче під'єднатися, і вихідний номер послідовності клієнта (у даному прикладі ISN, 1415531521). Це сегмент номер 1.

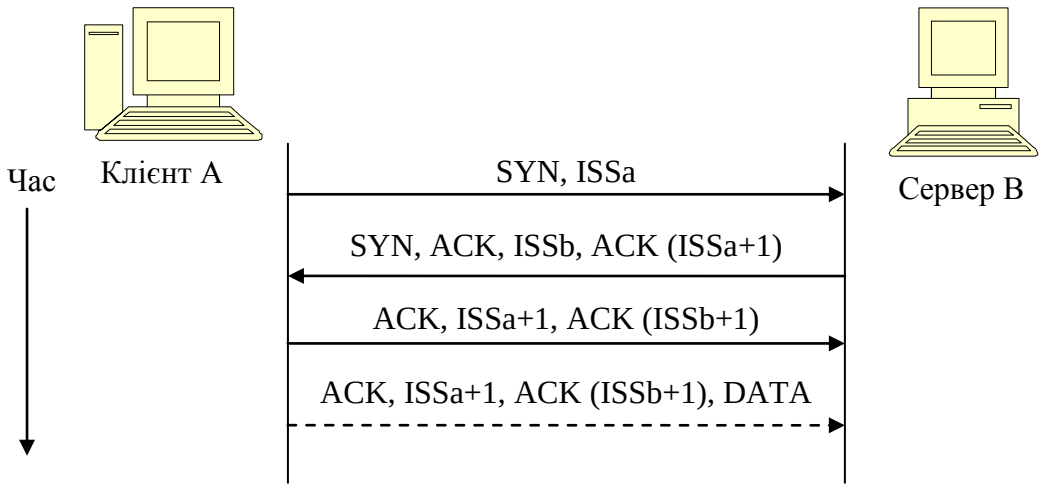


Рис. 3.11. Триступінчате рукостискання (three way handshake)

2. Сервер відповідає своїм сегментом SYN, що містить вихідний номер послідовності сервера (сегмент 2). Сервер також підтверджує прихід SYN клієнта з використанням ACK (ISN клієнта плюс одного). На SYN використовується один номер послідовності.
3. Клієнт повинен підтвердити прихід SYN від сервера з використанням ACK (ISN сервера плюс один, сегмент 3).

Цих трьох сегментів вистачає для встановлення з'єднання.

Вважається, що сторона, яка посилає перший SYN, активізує з'єднання (активне відкриття). Інша сторона, яка отримує перший SYN і відправляє наступний SYN, бере пасивну участь у відкритті з'єднання (пасивне відкриття).

Коли кожна сторона відправила свій SYN аби встановити з'єднання, вона вибирає вихідний номер послідовності (ISN) для цього з'єднання. ISN повинен мінятися кожного разу, тому кожне з'єднання має свій, відмінний від інших ISN. RFC 793 вказує, що ISN є 32-бітовим лічильником, який збільшується на одиницю кожні 4 мікросекунди. Завдяки номерам послідовностей, пакети, що затрималися в мережі і доставлені пізніше, не сприймаються як частина існуючого з'єднання.

Для того, щоб встановити з'єднання, необхідно 3 сегменти, а для того, щоб розірвати - 4. Це пояснюється тим, що TCP з'єднання може бути в наполовину закритому стані. Оскільки TCP з'єднання повнодуплексне (дані можуть пересуватися в кожному напрямі незалежно від іншого напряму), кожен напрям має бути закритий незалежно від іншого. Правило полягає в тому, що кожна сторона повинна послати FIN, коли передача даних завершена. Коли TCP приймає FIN, він повинен повідомити додаток, що віддалена сторона розриває

з'єднання і припиняє передачу даних в цьому напрямі. FIN зазвичай вирушає в результаті того, що додаток було закрите.

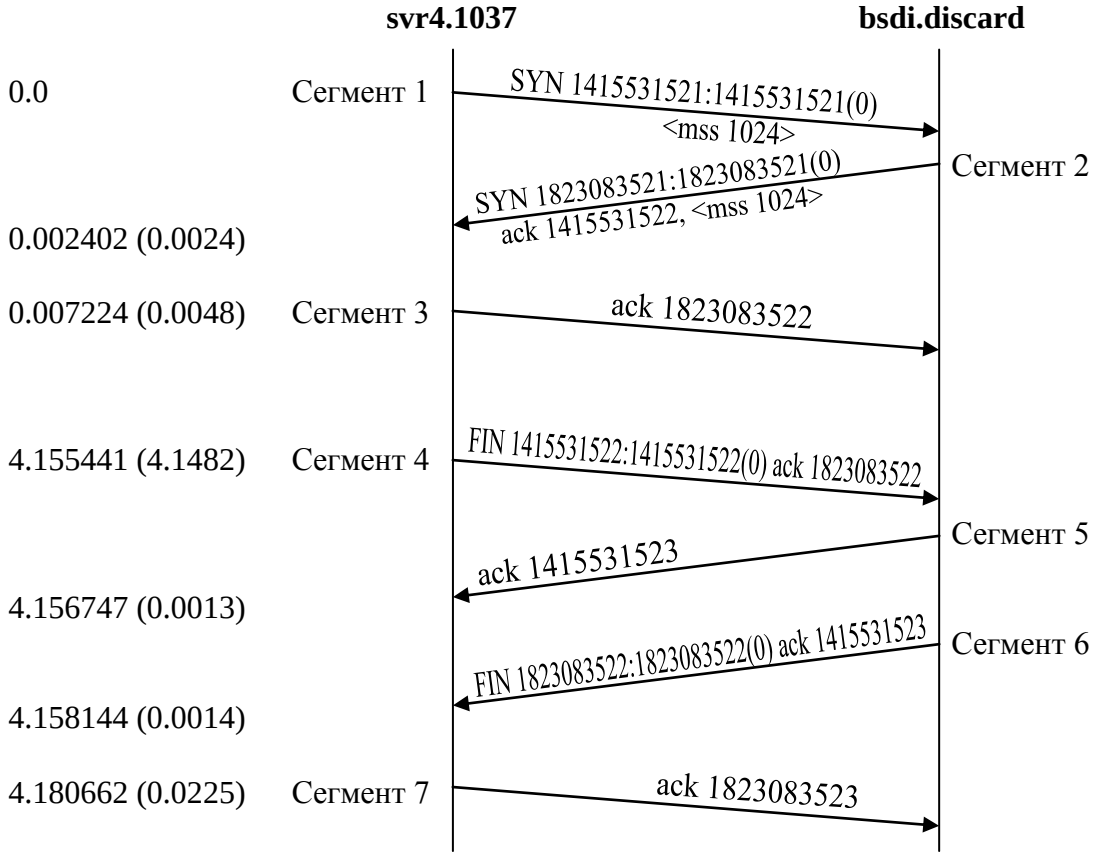


Рис. 3.12. Часова діаграма встановлення і розриву з'єднання.

Примітка. На часовій діаграмі використовується формат команди tcpdump. Запис 1415531521:1415531521 (0) означає, що номер послідовності пакету дорівнює 1415531521, а кількість байт даних в сегменті рівний 0.

Отримання FIN означає лише, що в цьому напрямі припиняється рух потоку даних. TCP, що отримав FIN, може все ще посилати дані. Не дивлячись на те, що додаток все ще може посилати дані при наполовину закритому з'єднанні TCP, на практиці лише деякі TCP - додатки використовують це. Звичайним є той сценарій, який показаний на рис. 3.12.

Можна сказати, що та сторона, яка першою закриває з'єднання (відправляє перший FIN), здійснює активне закриття, а інша сторона (яка прийняла цей FIN) здійснює пасивне закриття. Зазвичай, одна сторона здійснює активне закриття, а інша пасивне, проте інколи обоє сторони можуть здійснити активне закриття.

Хоча TCP- з'єднання є повнодуплексними, щоб зрозуміти, як відбувається їх роз'єднання, краще вважати їх парами симплексних з'єднань. Кожне симплексне з'єднання розривається незалежно від свого напарника. Аби

розірвати з'єднання, будь-яка із сторін може послати TCP-сегмент зі встановленим в одиницю бітом FIN, що означає, що у нього більше немає даних для передачі. Коли цей TCP-сегмент отримує підтвердження, цей напрям передачі закривається. Проте, дані можуть продовжувати передаватися невизначено довго в протилежному напрямі. З'єднання розривається, коли обидва напрями закриваються. Зазвичай для розриву з'єднання потрібно чотири TCP-сегмента: поодинці з бітом FIN і поодинці з бітом ACK в кожному напрямі. Перший біт ACK і другий біт FIN можуть також міститися в одному TCP-сегменті, що зменшить кількість сегментів до трьох.

Як при телефонній розмові, коли обоє учасника можуть одночасно попрощатися і повісити трубки, обоє кінця TCP- з'єднання можуть послати FIN-сегменти в один і той же час. Вони обоє отримують звичайні підтвердження, і з'єднання закривається. По суті, між одночасним і послідовним роз'єднаннями немає жодної різниці.

Для рішення цих проблем використовуються таймери. Якщо відповідь на посланий FIN-сегмент не приходить протягом двох максимальних інтервалів часу життя пакету, відправник розриває з'єднання. Інша сторона врешті-решт відмітить, що їй ніхто не відповідає, і також розірве з'єднання.

3.4.3. Управління потоком

Для прискорення і оптимізації процесу передачі великих об'ємів даних протокол TCP визначає метод управління потоком, який називається методом ковзаючого вікна, що дозволяє відправникові посилати черговий сегмент, не чекаючи підтвердження про отримання в пункті призначення попереднього сегменту.

Розглянемо базові принципи метода ковзаючого вікна. Протокол TCP формує підтвердження не для кожного конкретного успішно отриманого пакету, а для всіх даних від початку посилки до деякого порядкового номера ACK SN (Acknowledge Sequence Number).

Якщо ISN - початковий порядковий номер пакету (а точніше, байта), переданий під час встановлення з'єднання, SN - порядковий номер пакету, а ACK SN - порядковий номер підтвердження, то після встановлення з'єднання:

$$SN = ISN + 1$$

Якщо після встановлення з'єднання відправник передав декілька TCP-сегментів, в яких в цілому було передано n байт, то як підтвердження успішного прийому, перших n байт, висилається

$$ACK\ SN = SN + n + 1 = (ISN + 1) + n + 1$$

Це означає, що всі дані в байтовому потоці під номерами від *ISN+1* до *ISN+1+n* успішно отримані.

Разом з посилкою відправникові порядкового номера ACK SN одержувач оголошує також розмір вікна. Це означає, що відправник може посилати дані з порядковими номерами від поточного ACK SN до (ACK SN + розмір вікна - 1), не чекаючи підтвердження з боку одержувача. Якщо не буде отримано нове підтвердження (новий ACK SN), відправник посилатиме дані, поки він залишається в межах оголошеного вікна. Після цього посилка даних буде припинена до отримання чергового підтвердження і нового розміру вікна.

Розмір вікна вибирається так, щоб підтвердження встигали приходити вчасно і зупинки передачі не відбувалося. Розмір вікна може динамічно змінюватися одержувачем.

Для тимчасової зупинки посилки даних досить оголосити нульове вікно. Але навіть в цьому випадку через певні проміжки часу будуть від правляться сегменти з одним октетом даних. Це робиться для того, щоб відправник гарантовано дізнався про те, що одержувач знов оголосив ненульове вікно, оскільки одержувач зобов'язаний підтвердити отримання пробних сегментів, а в цих підтвердженнях він вкаже також і поточний розмір свого вікна. У протоколі TCP ковзаюче вікно використовується для регулювання трафіку і запобігання переповнюванню буфера.

Управління потоком даних за методом ковзаючого вікна (sliding window) дозволяє відправникові передати декілька пакетів, перш ніж він зупиниться і чекатиме підтвердження. При цьому дані передаються швидше, оскільки відправник не повинен зупинятися і чекати підтвердження кожного разу після відправки пакету.

Розглянемо приклад однобічної передачі 8192 байт від хоста svr4 до хосту bsdi [20].

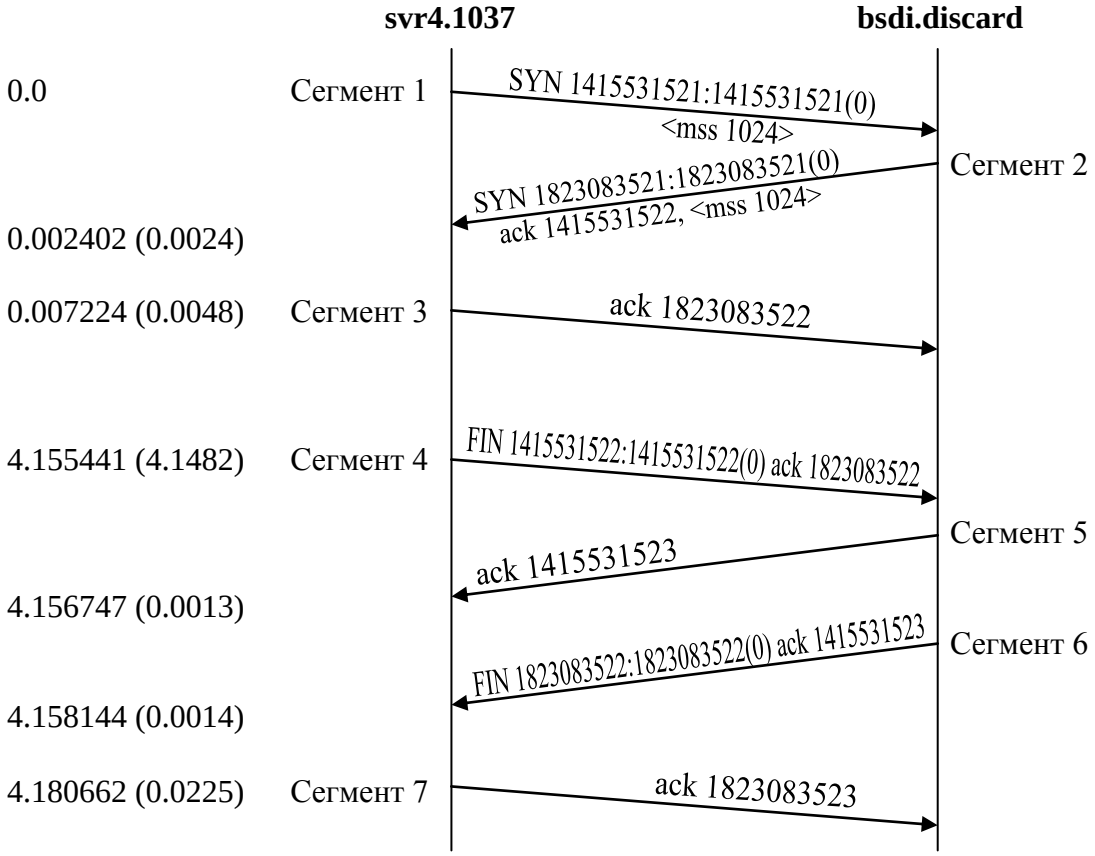


Рис. 3.13. Передавання 8192 байт від svr4 до bsdi.

Спочатку відправник передає три сегменти даних (4-6). Наступний сегмент (7) підтверджує лише перші два сегменти даних. Ми знаємо про це, тому що номер послідовності підтвердження дорівнює 2049, а не 3073.

Сегмент 7 містить ACK з номером 2049, а не 3073 з наступної причини. Коли пакет прибуває, він спочатку обробляється драйвером пристрою, а потім поміщається у вхідну чергу IP. Три сегменти 4, 5 і 6 прибувають один за дркгим і поміщаються у вхідну чергу IP в тому порядку, в якому вони були прийняті. IP потім передасть їх в TCP в тому ж самому порядку. Коли TCP обробляє сегмент 4, в з'єднанні генерується затриманий ACK. TCP обробляє наступний сегмент (5), і тепер TCP має два сегменти, на яких необхідно згенерувати підтвердження (ACK), тому генерується підтвердження з номером 2049 (сегмент 7), а прапор затриманого ACK для цього з'єднання знімається. TCP обробляє наступний вхідний сегмент (6), а в з'єднання знову генерується затриманий ACK. Перш ніж прибуває сегмент 9, вимикається таймер затриманого ACK і генерується підтвердження з номером 3073 (сегмент 8). У сегменті 8 вікно оголошується розміром 3072 байтів, оскільки 1024 байти даних в приймальному буфері TCP до цих пір не прочитано додатком.

В разі сегментів 11-16 підтвердження здійснюється на кожний сегмент. Сегменти 11, 12 і 13 прибувають і поміщаються у вхідну чергу IP. Коли сегмент 11 обробляється TCP, з'єднання позначається як використовуюче затриманий ACK. Коли обробляється сегмент 12, генерується ACK (сегмент 14) на сегменти 11 і 12, а прапор затриманого ACK для даного з'єднання знімається. При обробці сегменту 13 з'єднання знов позначається як використовуюче затриманий ACK, проте перш ніж затриманий ACK знімається по таймеру, обробляється сегмент 15, при цьому ACK (сегмент 16) вирушає негайно.

Порядок проходження пакетів, який ми бачимо, залежить від багатьох чинників, більшість з яких складно проконтролювати: реалізація посилаючого TCP, реалізація приймаючого TCP, читання даних приймаючим процесом (це залежить від процесу побудови часових графіків в операційній системі) і динаміки мережі (колізії в Ethernet). Не існує одного єдиного коректного способу для двох TCP здійснити обмін даними.

Протокол зміни розміру вікна, який ми розглянули в попередньому розділі, може бути проілюстрований таким чином (рис. 3.14).

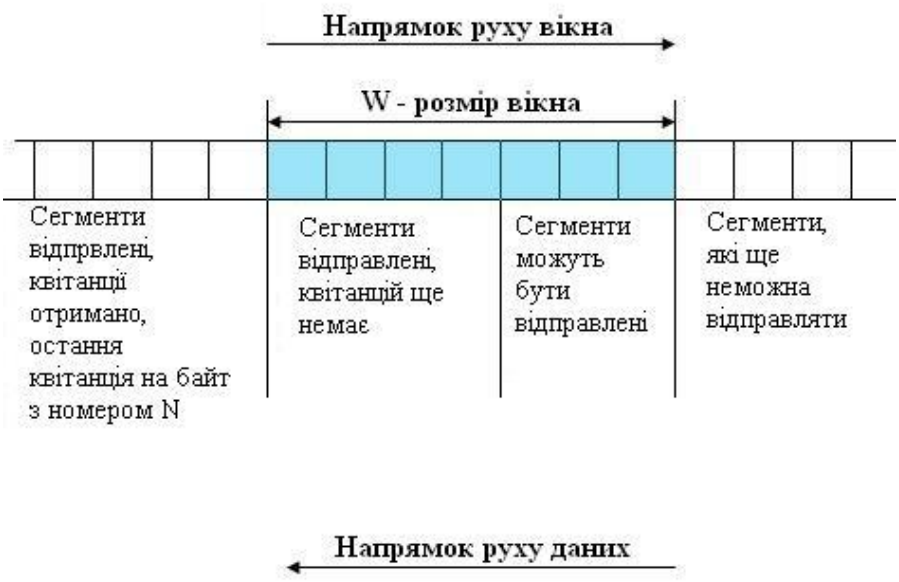


Рис. 3.14. Ілюстрація зміни вікна TCP.

На цьому рисунку байти пронумеровано з 1 по 11. Вікно, яке оголошується таким, що приймає, називається пропонованим вікном і покриває собою байти з 4 по 9, що означає, що одержувач підтвердив всі байти до 3 включно і оголошує розмір вікна рівний 6. Відправник розраховує свій можливий розмір вікна. Розраховане значення вказує, яку кількість даних він може відправити негайно.

З часом розмір вікна зрушується вправо, у міру того як одержувач підтверджує дані. Взаємне переміщення двох меж вікна збільшує або зменшує його розмір. Для опису переміщення меж вікна вправо і вліво використовуються три терміни.

1. Вікно закривається, коли його ліва межа збігається з правою. Це відбувається, коли дані відправлені і підтверджені.
2. Вікно відкривається, коли його права межа зрушується управо, при цьому дані можуть бути відправлені. Це відбувається, коли приймаючий процес читає підтверджені дані, звільняючи тим самим місце в приймальному буфері TCP.
3. Вікно стискується, коли його права межа пересувається вліво.

Якщо прийняті ACK, які вимагають переміщення лівої межі вікна вліво, це дубльовані ACK, вони відкидаються. Якщо ліва межа вікна збіглася з правою, це називається нульовим вікном. При цьому відправник припиняє передачу даних.

3.4.3.1. Механізм управління потоком - повільний старт. Алгоритм повільного старту полягає в тому, що здійснюється дослідження, з якою швидкістю нові пакети повинні відправлятися в мережу, причому ця швидкість повинна відповідати швидкості, з якою прийшли підтвердження з віддаленого кінця.

При роботі з повільним стартом відправляючому TCP додається ще одне вікно: вікно переповнювання (Congestion Window, CWnd). Коли встановлюється нове з'єднання з вузлом, що знаходиться в іншій мережі, розмір вікна переповнювання встановлюється рівним розміру одного сегменту MSS (розмір сегменту оголошений віддаленим кінцем). Кожного разу, коли приймається ACK, вікно переповнювання збільшується на один сегмент. (Розмір CWnd вимірюється в байтах, проте при повільному старті розмір завжди збільшується на розмір сегменту. Відправник може передати об'єм даних величиною до мінімального розміру вікна переповнювання і оголошеного вікна. За допомогою вікна переповнювання, відправник здійснює управління потоком, тоді як за допомогою оголошеного вікна потоком управляє одержувач.

Відправник починає роботу, відправивши один сегмент і чекаючи ACK на цей сегмент. Коли ACK отриманий, вікно переповнювання збільшується з одного сегменту до двох, і в цьому випадку можуть бути відправлені два сегменти. Коли кожен з цих двох сегментів підтверджений, вікно переповнювання збільшується до 4 (22). Таким чином, здійснюється експоненціальне збільшення.

У певній точці досягається максимум передачі для даного з'єднання (об'єднаній мережі), в цьому випадку проміжний маршрутизатор починає відкидати пакети.

Розглянемо, як використовується розмір вікна, як здійснюється управління потоком за допомогою вікон і повільного старту, а також як це впливає на пропускну спроможність TCP з'єднання, по якому передаються неінтерактивні дані (рис. 3.15).

У момент часу 0 відправник посилає один сегмент. Оскільки відправник працює з повільним стартом (вікно переповнювання встановлене в один сегмент), він повинен чекати підтвердження на цей сегмент, перш ніж продовжити роботу.

У моменти часу 1, 2 і 3 сегмент проходить по одному проміжку часу вправо. У момент часу 4 одержувач читає сегмент і генерує підтвердження. У моменти часу 5, 6 і 7 підтвердження рухається по одному проміжку часу вліво, назад до відправника. Таким чином, час повернення (RTT) складає 8 проміжків часу.

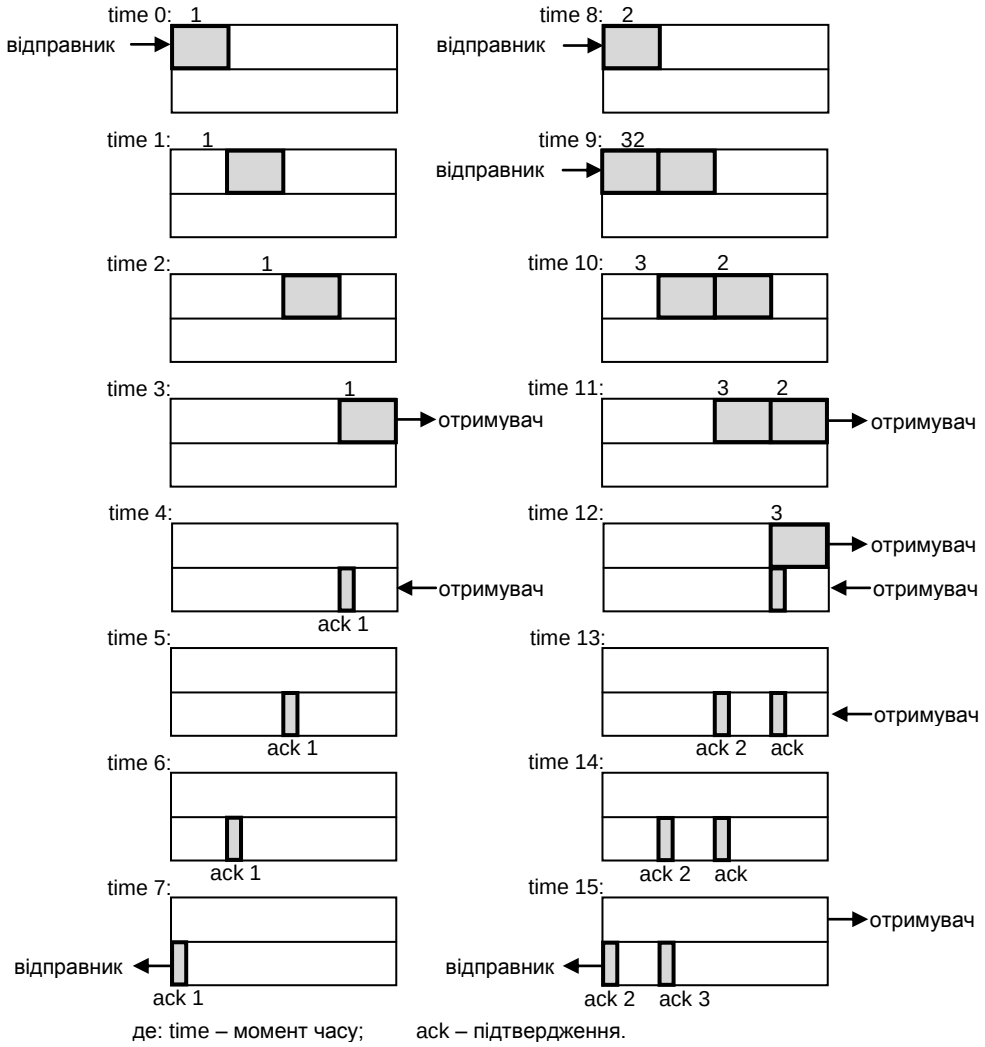


Рис. 3.15. Моменти часу 0-15, що ілюструють пропускну спроможність при передаванні даних.

Коли одержувач приймає ACK, він може передати два сегменти (які ми пронумерували як 2 і 3) в моменти часу 8 і 9. Вікно переповнювання зараз складає два сегменти. Ці два сегменти рухаються вправо у напрямку до приймача, де генеруються підтвердження в моменти часу 12 і 13. Проміжки часу між підтвердженнями (ACK) ідентичні проміжкам між сегментами даних. Це поведінка TCP називається самонастроюванням за часом (self-clocking). Оскільки одержувач може генерувати ACK лише тоді, коли дані отримані, по проміжках між підтвердженнями можна визначити швидкість прибуття даних до приймача.

Переповнювання може виникнути, коли дані прибувають з швидкого каналу (локальна мережа), а потім вирушають в повільний канал (глобальна мережа). Переповнювання також може виникнути, коли декілька вхідних потоків прибувають на маршрутизатор, вихідна пропускна спроможність якого менше ніж сума вхідних даних.

3.4.3.2. Алгоритм запобігання перевантаження. Регулювання трафіку в TCP має на увазі існування двох незалежних процесів: контролю доставки, керованого одержувачем за допомогою параметра Розмір вікна (Window), і контролю перевантаження, керованого відправником за допомогою Вікна перевантаження (Congestion Window, CWnd) і Порогу повільного старту (Slow Start Threshold, SSThreth).

Повільний старт - це спосіб спочатку встановити потік даних по з'єднанню. Проте, в цей же самий час ми досягнемо межі в проміжного маршрутизатора, при якому пакети відкидатимуться. Запобігання перевантаженню це спосіб, що дозволяє запобігти втраті пакетів.

Припущення, на якому будується алгоритм запобігання перевантаження, полягає в тому, що із-за різних пошкоджень втрачається дуже мале число пакетів (значно менше ніж 1%), тому втрата пакетів сигналізує про те, що в якому-небудь місці мережі між джерелом і призначенням з'явилося перевантаження. Існують дві ознаки, по яких можна визначити, що пакети втрачаються: поява тайм-аутів (підтвердження не повертається в строк) і отримання дубльованих ACK

Запобігання перевантаження (переповнювання) і повільний старт це незалежні один від одного алгоритми, більш того, працюють з різними об'єктами. Проте, коли виникає перевантаження, необхідно уповільнити швидкість передачі пакетів по мережі, а потім використовувати повільний старт, аби почати все з початку. На практиці ці алгоритми використовуються разом.

Необхідно визнати існування двох потенційних проблем: низькій пропускній спроможності мережі і низької ємкості одержувача. Для цього у кожного відправника є два вікна: вікно, надане одержувачем, і вікно

перевантаження CWnd. Розмір кожного з них відповідає кількості байтів, яка відправник має право передати.

Відправник керується мінімальним з цих двох значень. Наприклад, одержувач говорить: «Посилайте 8 Кбайт», але відправник знає, що якщо він пошле більше 4 Кбайт, то в мережі утворюється затор, тому він посилає все ж 4 Кбайт. Якщо ж відправник знає, що мережа здатна пропустити і більшу кількість даних, наприклад 32 Кбайт, він передасть стільки, скільки просить одержувач (тобто 8 Кбайт).

При установці з'єднання відправник встановлює розмір вікна перевантаження рівним розміру максимального використовуваного в даному з'єднанні сегменту. Потім він передає один максимальний сегмент. Якщо підтвердження отримання цього сегменту прибуває перш, ніж витікає період чекання, до розміру вікна додається розмір сегменту, тобто розмір вікна перевантаження подвоюється, і посилаються вже два сегменти.

У відповідь на підтвердження отримання кожного з сегментів проводиться розширення вікна перевантаження на величину розміру поточного вікна. Допустимо, розмір вікна дорівнює *n* сегментам. Якщо підтвердження для всіх сегментів приходять вчасно, вікно збільшується на число байтів, відповідне *n* сегментам. По суті, підтвердження кожної послідовності сегментів призводить до подвоєння вікна перевантаження.

Цей процес експоненціального зростання продовжується до тих пір, поки не буде досягнутий розмір вікна одержувача або не буде вироблена ознака таймауту, що сигналізує про перевантаження в мережі. Наприклад, якщо пакети розміром 1024, 2048 і 4096 байт дійшли до одержувача успішно, а у відповідь на передачу пакету розміром 8192 байти підтвердження не прийшло у встановлений термін, вікно перевантаження встановлюється рівним 4096 байтам. Поки розмір вікна перевантаження залишається рівним 4096 байтам, довші пакети не посилаються, незалежно від розміру вікна, що надається одержувачем. Цей алгоритм називається повільним стартом. Проте він не такий вже і повільний. Він експоненціальний. Всі реалізації протоколу TCP зобов'язані його підтримувати.

Запобігання перевантаженню і повільний старт вимагають, аби для кожного з'єднання були визначені дві змінні: вікно перевантаження, *CWnd*, і розмір порогу повільного старту, *SSThresh*.

Таким чином, окрім вікон одержувача і перевантаження, як третій параметр в нім використовується порогове значення, яке спочатку встановлюється рівним 64 Кбайт. Коли виникає ситуація таймауту (підтвердження не повертається в строк), нове значення порогу встановлюється рівним половині поточного розміру вікна перевантаження, а вікно

перевантаження зменшується до розміру одного максимального сегменту (рис.3.16)

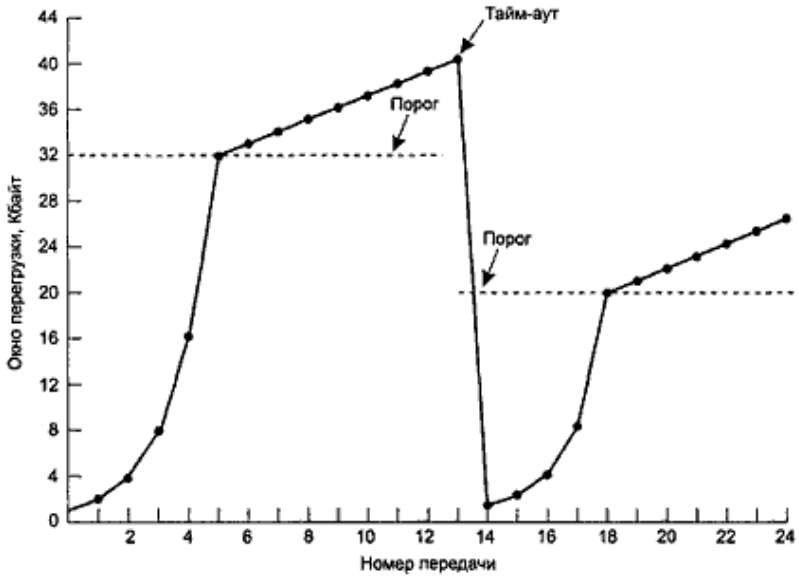


Рис. 3.16 - Приклад функціонування механізму запобігання перевантаження

Потім, так само як і у попередньому випадку, використовується алгоритм повільного старту, що дозволяє швидко виявити межу пропускної спроможності мережі. Проте цього разу експоненціальне зростання розміру вікна зупиняється після досягнення ним порогового значення, після чого вікно збільшується лінійно, на один сегмент для кожної наступної передачі. По суті, передбачається, що можна урізувати удвічі розмір вікна перевантаження, після чого поступово нарощувати його.

Приклад, приведений на рис. 3.16 ілюструє цей алгоритм: максимальний розмір сегменту дорівнює 1024 байт. Спочатку вікно перевантаження було встановлене рівним 64 Кбайт, але потім стався таймаут, і поріг став рівним 32 Кбайт, а вікно перевантаження — 1 Кбайт (передача 0). Потім розмір вікна перевантаження подвоюється на кожному кроці, поки не досягає порогу (32 Кбайт). Починаючи з цього моменту, розмір вікна збільшується лінійно.

Передача 13 виявляється невдалою, оскільки спрацьовує таймаут. При цьому порогове значення встановлюється рівним половині поточного розміру вікна (40 Кбайт навпіл, тобто 20 Кбайт), і знову відбувається повільний старт. Після досягнення порогового значення експоненціальне зростання розміру вікна змінялося лінійним.

Якщо таймаутів більше не виникає, вікно перевантаження може продовжувати зростати до розміру вікна одержувача. Потім зростання

припиниться, і розмір вікна залишиться постійним, поки не станеться таймаут або не зміниться розмір вікна одержувача.

Таким чином, алгоритм управління перевантаженням може бути представлений у вигляді наступної послідовності кроків:

Крок 1. Ініціалізація змінних: вікно переповнювання заданого з'єднання *CWnd* встановлюється рівним одному сегменту (MSS); а розмір порогу повільного старту *SSThresh* дорівнює 65535 байт.

Крок 2. Порівняння значень вікна переповнювання *CWnd* і вікна, що оголошене одержувачем (Window). Вибирається менше значення.

Крок 3. Пересилка даних і отримання підтвердження.

Крок 4. Якщо отримання чергового блоку даних підтверджене без виділення таймауту, значення *CWnd* збільшується (подвоюється).

Крок 5. Якщо підтвердження не отримане в строк, нове значення порогу встановлюється рівним половині поточного розміру вікна перевантаження, а вікно перевантаження зменшується до розміру одного максимального сегменту, тобто запускається процедура повільного старту. Вікно перевантаження подвоюється на кожному кроці, поки не досягає порогу *SSThresh*. Коли цей рівень *CWnd* досягнутий, подальше зростання відбувається лінійно з приростом на кожному кроці, рівному MSS.

Запобігання переповнюванню це спосіб контролювати потік даних, з боку відправника, тоді як оголошення вікна це спосіб контролювати потік даних, з боку одержувача. Перший процес відстежує заповнення вхідного буфера одержувача, другий - реєструє перевантаження каналу і пов'язані з цим втрати, а також знижує інтенсивність трафіку.

Контрольні запитання

1. Яка роль ковзаючого вікна в протоколі TCP?
2. Опишіть поле Тип обслуговування IP- заголовка.
3. Назвіть алгоритми управління потоком в протоколі TCP.
4. Опишіть алгоритм повільного старту в протоколі TCP.
5. Скільки байт містить IP-адрес (версії v4)?
6. Сформулюйте головну функцію транспортного рівня еталонної моделі OSI.
7. Який рівень еталонної моделі OSI вирішує питання повідомлення про несправності, враховує топологію мережі і управляє доступом до середовища передачі даних?

8. Для чого використовується поле Розмір вікна TCP - заголовка?
9. Сформулюйте принцип інкапсуляції даних.
10. Порівняєте еталонну модель OSI з ієрархією стека TCP/IP.
11. Для чого використовується псевдозаголовок TCP?
12. Сформулюйте основні етапи алгоритму триступінчатого рукостискання.
13. IP-адрес хост-машини - 192.168.5.121, маска підмережі - 255.255.255.248. Який адрес має мережа цього хоста?
14. Яка частина IP-адреса 205.129.12.5 представляє хост-машину?
15. Яка частина адреса 182.54.4.233 визначає підмережу?
16. Визначити, є IP-адрес 192.168.155.128/25 адресом мережі або адресом хоста?
17. Якщо мережа класу B розділена на підмережі і має маску 255.255.240.0, то яку максимальну кількість підмереж можна створити?
18. Якщо мережа має маску 255.255.240.0, то яку максимальну кількість вузлів можна підключити для заданої мережі?

Розділ 4. Рівень транспорту. Транспортні мережі MPLS

4.1 Узагальнена структура MPLS

Багатопротокольна комутація по мітках MPLS (Multiprotocol Label Switching) – технологія, розроблена робочою групою по створенню інтегрованих послуг IETF. Це нова архітектура побудови магістральних мереж, яка значно розширює перспективи масштабування, підвищує швидкість обробки трафіку і надає величезні можливості для організації додаткових послуг. Технологія MPLS поєднує в собі можливості управління трафіком, властиві технологіям канального рівня, і масштабованість і гнучкість протоколів, характерні для мережного рівня. Будучи результатом злиття механізмів різних компаній, вона ввібрала в себе найбільш ефективні рішення кожній. MPLS з'єднала в собі надійність ATM, зручні і потужні засоби доставки і забезпечення гарантованої якості обслуговування IP-мереж, – така інтеграція мереж дозволяє отримати додаткову вигоду із спільного використання протоколів IP і ATM [2].

Головна особливість технології MPLS – відділення процесу комутації пакету від аналізу IP-адреса в його заголовку, що дозволяє здійснювати комутацію пакетів значно швидше. Відповідно до протоколу MPLS маршрутизатори привласнюють кожній точці входу в таблицю маршрутизації особливу мітку і повідомляють цю мітку сусіднім пристроям. Наявність таких міток дозволяє маршрутизаторам і комутаторам, що підтримують технологію MPLS, визначати наступний крок в маршруті пакету без виконання процедури пошуку адреса. На сьогоднішній день існують три основні сфери застосування MPLS:

- управління трафіком;
- підтримка класів обслуговування (CoS);
- організація віртуальних приватних мереж (VPN).

Розташування технології MPLS в семирівневій моделі OSI (Open Systems Interconnection) показане на рис. 4.1. "Multiprotocol" в назві технології означає "багатопротокольний". Це говорить про те, що технологія MPLS застосовна до будь-якого протоколу мережного рівня, тобто MPLS – це свого роду інкапсулюючий протокол, здатний транспонувати інформацію множині інших протоколів вищих рівнів моделі OSI. Таким чином, технологія MPLS залишається незалежною від протоколів рівнів 2 і 3 в мережах IP, ATM і Frame Relay, а також взаємодіє з існуючими протоколами маршрутизації, такими як протокол резервування ресурсів RSVP або мережний протокол переважного вибору найкоротших маршрутів OSPF [4].

Площина пересилки даних MPLS відповідає за перенаправлення пакетів у відповідності до значень, що містяться в мітках. Площина пересилки даних MPLS не утворює повноцінного рівня, вона "уклинюється" в мережі IP, ATM або Frame Relay між 2-м і 3-м рівнями моделі OSI, залишаючись незалежною від цих рівнів. Можна сказати, що одночасне функціонування MPLS на мережному рівні і на рівні ланки даних наводить до утворення так званого рівня 2.5, де, власне, і виконується комутація по мітках. Площина управління відповідає за формування і підтримку інформаційної бази міток [22].

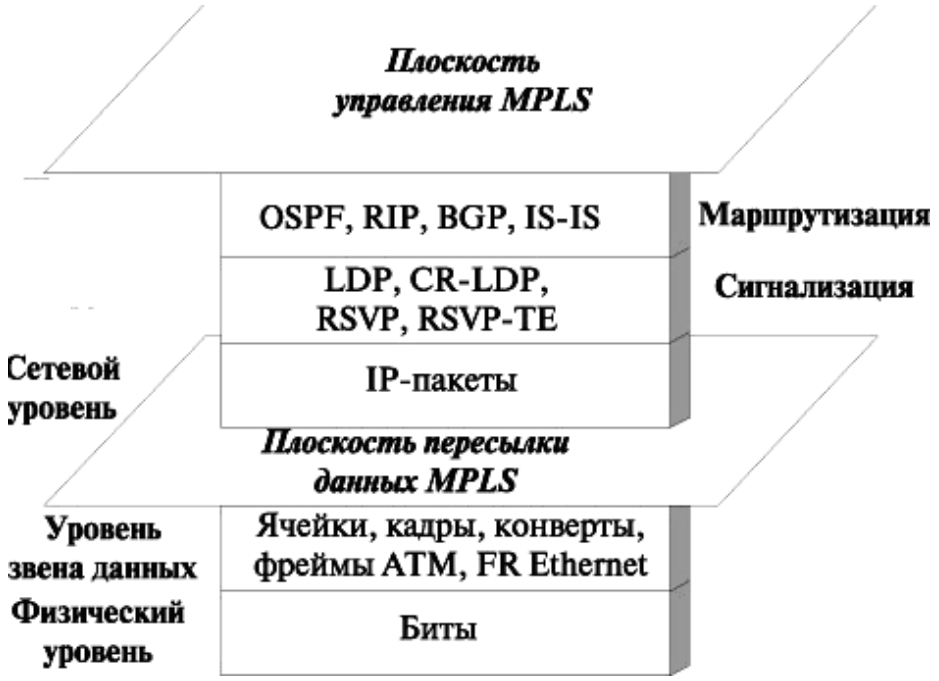


Рис. 4.1 – Площини MPLS

Всі вузли середовища MPLS повинні використовувати протокол маршрутизації IP для обміну відповідною інформацією маршрутизації з іншими вузлами MPLS мережі. Наприклад, вузли середовища ATM з функціями MPLS використовують зовнішній контролер комутації по мітках (Label Switch Controller – LSC).

4.2 Базові поняття технології MPLS

Базовими поняттями технології MPLS є:

- мітка (Label);
- FEC (Forwarding Equivalence Class) – клас еквівалентності пересилки;
- LSP (Label Switched Path) – комутований по мітках тракт (маршрут);
- LSR (Label Switching Router) – маршрутизатор комутації по мітках;
- LDP (Label Distribution Protocol) – протокол розподілу міток.

Для пересилки пакетів в мережах MPLS використовуються мітки. Вхідний вузол мережі MPLS відносить пакет до певного класу еквівалентності при пересилці лише один раз – у момент надходження в мережу.

4.2.1 Клас еквівалентності пересилки FEC

Клас еквівалентності пересилки FEC – це форма представлення групи пакетів (які є сімейством пакетів 3-го рівня) з однаковими вимогами до передачі, тобто всі пакети такої групи обробляються однаково на шляху їх прямування до пункту призначення.

При традиційній IP-маршрутизації конкретний маршрутизатор теж може вважати, що два пакети належать одному і тому ж умовному класу еквівалентності, якщо в його таблицях маршрутизації використовується деякий адресний префікс, що ідентифікує напрям, в якому передбачувані маршрути транспортування цих двох пакетів збігаються найдовше. У міру просування пакету по мережі кожен наступний маршрутизатор аналізує його заголовок і приписує цей пакет до того з власних (таких, що належать лише цьому маршрутизатору) класів еквівалентності, який відповідає тому ж напряму. На відміну від традиційної маршрутизації, при використанні багатопротокольної комутації на основі міток пакет ставиться у відповідність певному класу FEC лише один раз на вході в мережу MPLS. Цьому FEC привласнюється мітка, яка передається потім разом з пакетом при його пересилці до наступного маршрутизатора. У решти маршрутизаторів заголовок пакету не аналізується. Визначення FEC реалізується на основі вимог до обслуговування даної сукупності пакетів або просто адресного префікса. Таким чином, прикладом FEC можуть служити всі IP-пакети з адресами пунктів призначення, відповідними деякому префіксу, наприклад 223.18.6. Можливі також FEC на основі префікса адреса і ще якого-небудь поля IP-заголовка, наприклад тип обслуговування (ToS).

При відношенні пакету до деякого класу еквівалентності FEC маршрутизатор може проглянути IP-заголовок пакету, а також використовувати іншу інформацію, зокрема номер інтерфейсу, на який поступив пакет. Клас FEC може здійснювати "тонше" або "грубіше" сортування пакетів (розподіл пакетів по класах) залежно від кількості інформації, яка розглядалася при призначенні пакету його класу еквівалентності [22].

Наприклад, класи FEC можуть формуватися як:

- Набор пакетів, в яких адрес одержувача 3-го рівня відповідає адресному префіксу.
- Набор пакетів, в яких адрес одержувача відповідає заданому префіксу IP-адреса і, в яких співпадають біти типа обслуговування (Type of Service — TOS);
- Набор пакетів, в яких адрес одержувача відповідає заданому префіксу IP-адреса і, які мають один і той же номер TCP-порту пункту призначення;

- Набор пакетів багатоадресної розсилки з одними і тими ж адресами 3-гоуровня відправника і одержувача.

При співвідношенні пакетів по різних FEC велику роль грають IP-адреса, пріоритети обслуговування і інші параметри трафіку. Кожен FEC обробляється окремо, що дозволяє підтримувати необхідну якість обслуговування в мережі MPLS.

Метод пересилки пакетів на основі пар " FEC -метка", прийнятий в MPLS, має ряд переваг перед методами, заснованими на аналізі заголовка блоків мережного рівня. Зокрема, пересилку за методом MPLS можуть виконувати маршрутизатори, які здатні читати і замінювати мітки, але при цьому або взагалі не здатні аналізувати заголовки блоків мережного рівня, або не здатні робити це достатньо швидко.

4.2.2 Мітка

Мітка – це ідентифікатор фіксованої довжини, що визначає клас еквівалентності пересилки FEC. Мітки мають локальне значення, тобто прив'язка мітки до FEC використовується лише для пари маршрутизаторів. Мітка використовується для пересилки пакетів від верхнього маршрутизатора до нижнього, де, будучи вхідною, замінюється на вихідну мітку, що має також локальне значення на наступній ділянці маршруту. Мітка передається у складі будь-якого пакету, при цьому її місце в пакеті залежить від використовуваної технології канального рівня.

Протокол MPLS підтримує різні типі міток: це може бути 4-байтова мітка, яка вставляється між заголовками канального і мережного рівня. Будучи протокольно незалежною, вона може використовуватися для інкапсуляції пакетів будь-якого протоколу мережного рівня. Це може бути мітка ідентифікаторів віртуального каналу і віртуального шляху (VCI/VPI) або мітка ідентифікатора з'єднання канального рівня (DLCI).

Розмір мітки складає 4 байти. Формат мітки приведений на рис. 4.2.

Мітка містить наступні поля:

- *Label field* - 20-ти бітове поле ідентифікатора мітки. Може бути будь-яким числом в діапазоні від 0 до (2^{20}-1), за винятком резервних значень (0, 1, 2, 3 і ін.), визначенням використання яких займається робоча група MPLS у складі комітету IETF.
- *CoS field* - 3-х бітове поле класу обслуговування - задає алгоритм черговості і відкидання пакетів при передачі.
- *Stack field* - 1-бітове поле стека
- *TTL (time to live) field* - 8-мі бітове поле часу існування - виконує функції поля *TTL* в IP, тобто є механізмом, що запобігає можливості нескінченної циркуляції пакетів по мережі унаслідок утворення закольцованих маршрутів. Байт *TTL* знаходиться в кінці заголовка мітки.

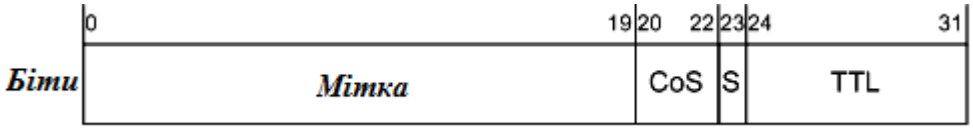


Рис.4.2-Формат мітки MPLS

Коли отриманий помічений пакет, аналізується значення мітки нагорі стека. В результаті цього аналізу визначається:

- наступний крок, куди має бути переадресований пакет;
- операція, яка має бути виконана із стеком міток до переадресації. Ця операція може бути заміною мітки на вершині стека, або видаленням запису із стека, або заміщенням верхньої позиції в стеку і занесенням туди потім одній або новіших записів.

Існує декілька зарезервованих значень міток, які наведено в таблиці 4.1.

Таблиця 4.1 – Зарезервовані значення міток

Значення	Опис
0	Явно задана нульова мітка протоколу IPv4: "IPv4 Explicit NULL Label". Це значення мітки є єдино допустимим для дна стека міток. Воно вказує, що стек має бути очищений і переадресація пакету повинна грунтуватися на IPv4-заголовке.
1	Мітка попередження маршрутизатора: "Router Alert Label". Це значення мітки є легальним в будь-якому місці стека міток, за винятком дна. Використання цієї мітки схоже із застосуванням опції "Router Alert" в IP-пакетах.
2	Явно задана нульова мітка протоколу IPv6: "IPv6 Explicit NULL Label". Це значення мітки є єдино допустимим для запису на дні стека. Воно вказує, що стек має бути очищений, а переадресація пакетів повинна після цього грунтуватися на заголовку IPv6.
3	Неявно задана нульова метка"Implicit NULL Label". Це мітка, яку LSR може привласнювати і розсилати, але яка насправді ніколи не використовується при інкапсуляції.
4–15	Зарезервовані

Пакет, що передається по мережі MPLS, як правило, містить не одну, а декілька міток. Такий набір міток утворює стек. Для вказівки кінця стека відповідний біт встановлюється в 1, всім останнім бітам стека задається значення 0. Початок стека знаходиться відразу після заголовка канального рівня, а кінець - відразу перед заголовком мережного. Пересилка пакетів

використовується за значенням мітки на початку стека. Стек використовується для VPN-мереж і при перерозподілі потоків. Основне призначення стека міток – підтримка деревоподібності множини маршрутів LSP, що закінчуються в одному вхідному LSR, а, крім того, в тому, аби використовувати мітки при створенні так званих LSP - тунелів.

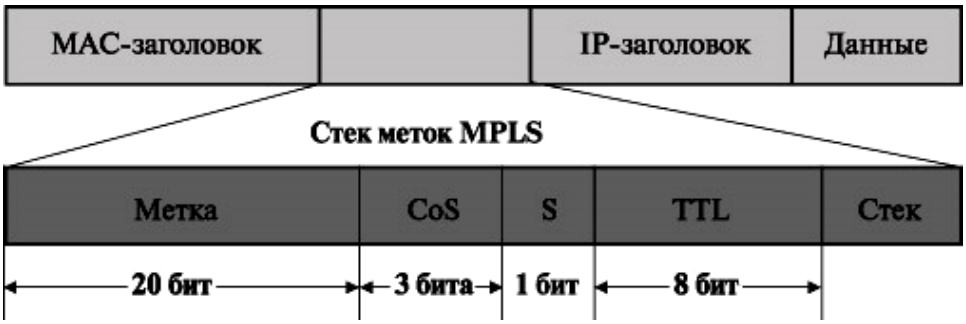


Рис. 4.3 - Формат запису стека міток

Можливість мати в пакеті більш за одну мітку у вигляді стека дозволяє створювати ієрархію міток, що відкриває шлях багатьом додаткам (RFC3032 "MPLS Label Stack Encoding"). MPLS може виконати із стеком наступні операції: поміщати мітку в стек, видаляти мітку із стека і замінювати мітку. Ці операції можуть використовуватися для злиття і розгалуження інформаційних потоків. Операція розміщення мітки в стек (push operation) додає нову мітку поверх стека, а операція видалення мітки із стека (pop operation) видаляє верхню мітку стека. Функціональні можливості стека MPLS дозволяють об'єднувати декілька LSP в один. До стека міток кожного з цих LSP зверху додається загальна мітка, внаслідок чого утворюється агрегований тракт MPLS. У точці закінчення такого тракту відбувається його розгалуження на складаючі його індивідуальні LSP. Так можуть об'єднатися тракти, що мають загальну частину маршруту. Отже, MPLS здатна забезпечувати ієрархічну пересилку, що може стати важливою та необхідною функціональною можливістю. При її використанні не потрібно переносити глобальну маршрутну інформацію, і це робить мережу MPLS більш стабільною і масштабованою, чим мережа з традиційною маршрутизацією.

Згідно правилам інкапсуляції міток, що розглядаються нижче, за міткою MPLS в пакеті завжди повинен слідувати заголовок мережного рівня. Оскільки MPLS починає роботу верхнього рівня стека, цей стек використовується за принципом LIFO "останнім прийшов, першим пішов". Приклад чотирьохрівневого стека міток представлений на рис.4.4.

Заголовок MPLS № 1 був першим заголовком MPLS, розташованим в пакеті, потім в нього були поміщені заголовки № 2, № 3 і, нарешті, заголовок № 4. Комутація по мітках завжди використовує верхню мітку стека, і мітки видаляються з пакету так, як це визначено вихідним вузлом для кожного LSP, по якому слідує пакет. Біт S має значення 1 в нижній мітці стека і 0 – у всіх останніх мітках. Це дозволяє прив'язувати префікс до декількох міток, іншими словами – до стека міток (Label Stack)

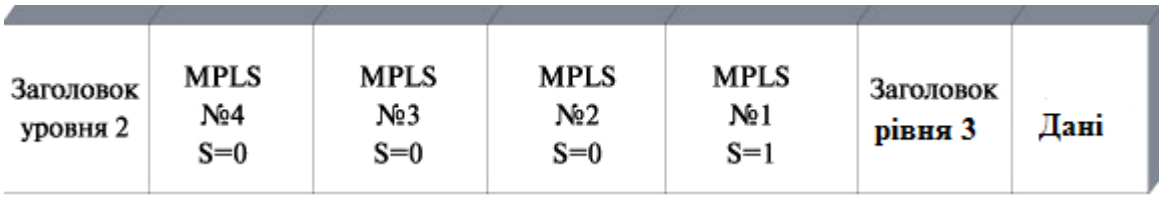


Рис. 4.4 – Чотирьохрівневий стек міток

При використанні протоколів комутації на рівні ланки даних, таких як ATM і Frame Relay, верхня MPLS-мітка вписується в поле ідентифікаторів цих протоколів, причому, при використанні ATM для розміщення MPLS-мітки використовується поле VPI/VCI, а при використанні Frame Relay – поле DLCI (Data Link Connection Identifier). У тих випадках, коли MPLS забезпечує пересилку IP-пакетів мережного рівня і, коли технологія рівня ланки даних не підтримує власне поле міток, MPLS-заголовок повинен інкапсулюватися між заголовками рівня ланки даних і мережного рівня.

Механізм інкапсуляції переносить дані протоколів верхніх рівнів як корисне навантаження в дейтаграмі інкапсулюючого протоколу. По суті, вводиться новий заголовок, який робить з інкапсульованого заголовка і поля даних нове поле даних. Загальна модель інкапсуляції представлена на рис. 4.5, де вважається, що інкапсуляція MPLS може бути використана з будь-якою технологією рівня 2. Мітка MPLS може бути поміщена в існуючий формат заголовка рівня 2, як в разі ATM або FR, або вписана в спеціальний заголовок MPLS, як в разі Ethernet або PPP. У всіх випадках будь-які додаткові мітки знаходяться між верхньою міткою стека і IP-заголовком рівня 3. Показаний на рис 4.5 заголовок MPLS часто називають shim header ("заголовком - клином"), підкреслюючи в метафоричній формі той факт, що цей заголовок уклинюється в пакет між заголовками рівня даних і мережного рівня, тобто створює рівень 2.5.

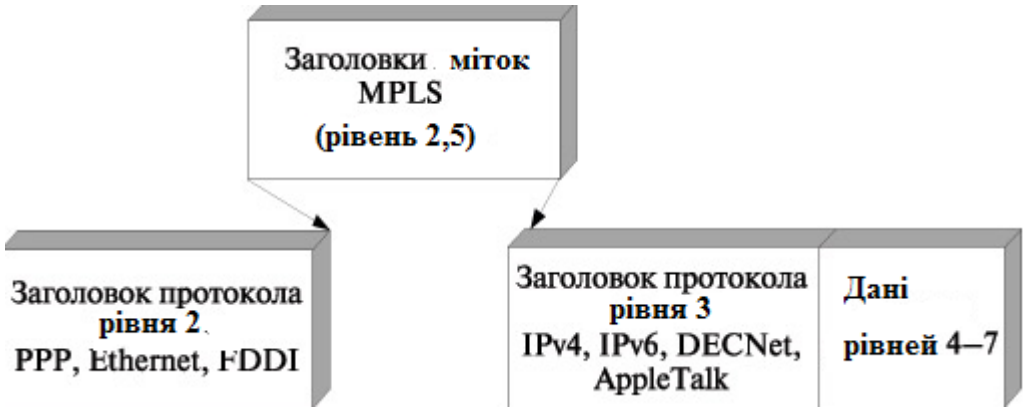


Рис. 4.5 – Принцип інкапсуляції заголовка MPLS

Однією з найсильніших сторін технології MPLS є те, що вона може використовуватися спільно з різними протоколами рівня 2. Серед цих

протоколів – ATM, Frame Relay, PPP і Ethernet, FDDI та інші, передбачені нормативними документами по MPLS.

Розглянемо, як мітка може вписуватися в заголовок рівня ланки даних (VCI/VPI для мережі ATM, DLCI для мережі Frame Relay і тому подібне) або "вставлятися" між заголовками рівня ланки даних і мережного рівня. Із самого початку робоча група IETF MPLS вирішила, що у всіх випадках, коли це можливо, MPLS повинна використовувати існуючі формати. З цієї причини інформація мітки MPLS може передаватися в пакеті декількома різними методами:

- як частина заголовка другого рівня ATM, коли інформація мітки передається в ідентифікаторах віртуального каналу VCI і віртуального тракту VPI (рис. 4.6);
- як частина кадру AAL5 рівня адаптації ATM (ATM Adaptation Layer 5) перед сегментацією і збіркою SAR (Segmentation and Reassembly), що виконується в середовищі ATM у разі, коли ця інформація містить дані про стек міток (декілька полів MPLS-міток);
- як частина заголовка другого рівня Frame Relay, коли інформація мітки передається в ідентифікаторах DLCI, що показано на рис. 4.7;
- як нова 4-байтова мітка, звана клином (shim), яка вставляється між заголовками другого і третього рівнів (рис. 4.8), – у всіх останніх випадках.

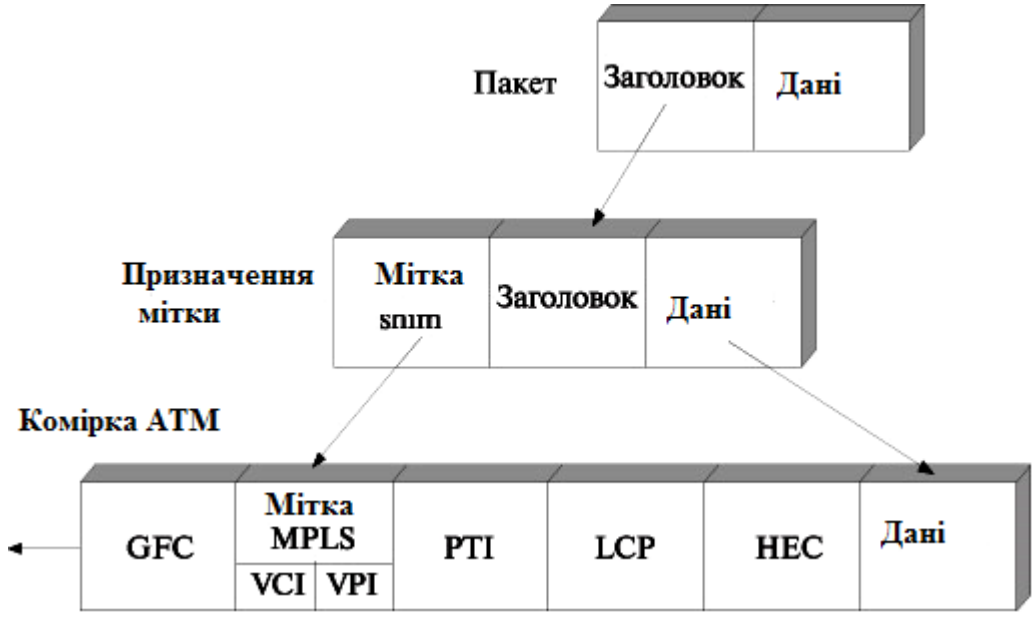


Рис. 4.6 - MPLS-мітка в полях VPI/VCI заголовка ATM

Використання MPLS зверху ATM досить поширене для транспортування по мережах ATM трафіку IP. ATM-комутатори, які сконфігуровано для підтримки MPLS (ATM-LSR), виконують протоколи маршрутизації TCP/IP і використовують пересилку даних в чарунках ATM фіксованої довжини (53 байти). Усередині цих комутаторів верхня мітка MPLS розміщується в поля

VCI/VPI заголовка чарунки ATM, а дані про стек міток MPLS – в полі даних чарунок ATM.

Подібно до ATM, FR-комутатори, що підтримують MPLS, застосовують протоколи маршрутизації TCP/IP для пересилки даних під управлінням FR. При використанні FR поточна мітка розміщується в полі ідентифікатора каналу ланки даних DLCI в заголовку FR. Будь-які додаткові записи в стек міток MPLS переносяться після заголовка FR, але до заголовка мережного рівня, що міститься в полі даних кадру FR. Стандарт MPLS дозволяє FR використовувати адресу Q.922 завдовжки або 2 октети, або 4 октети. Формат представлений на рис. 4.7.

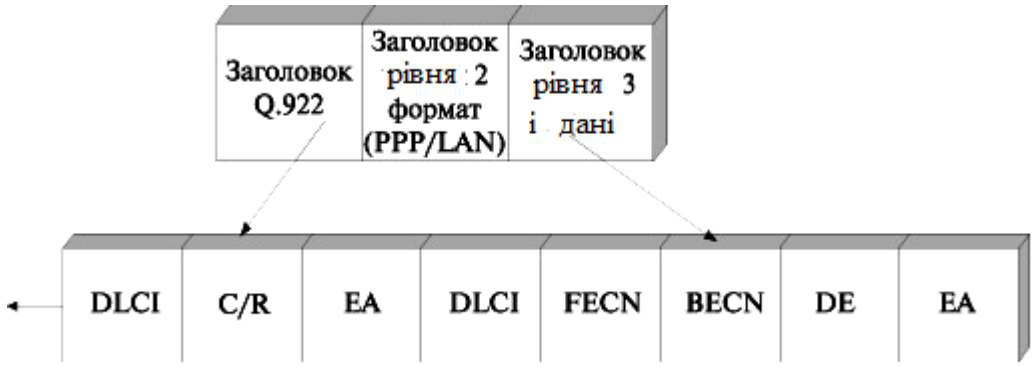


Рис. 4.7 – Розміщення мітки MPLS в кадрі FR

Відносно чарунок ATM і кадрів Frame Relay домовилися використовувати для MPLS існуючі формати заголовків, а у всіх інших випадках – власну мітку MPLS між заголовками другого і третього рівнів. Звідси видно, що MPLS дозволяє створювати нові формати міток без зміни протоколів маршрутизації, а тому ця технологія може застосовуватися і для інших видів оптичного транспорту (щільне мультиплексування з розділенням по довжині хвилі DWDM (Dense Wave Division Multiplexing) і оптична комутація).

Цей же принцип інкапсуляції використовується також для каналів типа "точка-точка" (Point-to-Point – PPP) і для локальних мереж Ethernet (рис. 4.8).

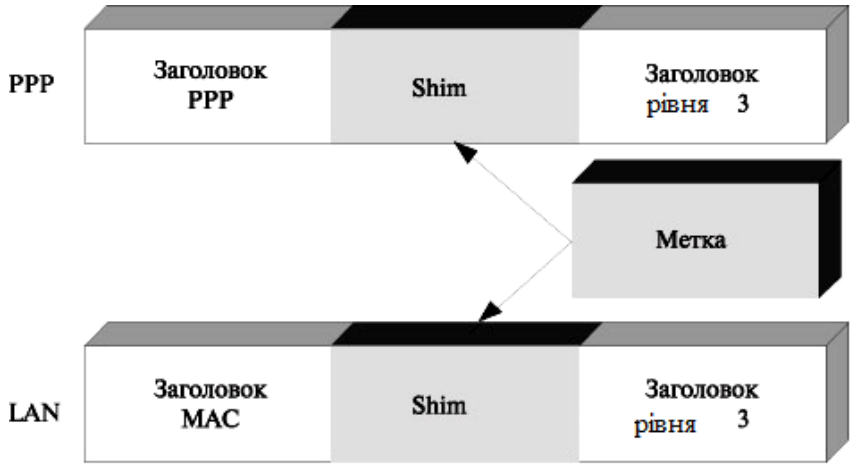


Рис. 4.8 - Формат для введення MPLS-мітки в пакет PPP і в кадр Ethernet

Коли пакети MPLS передаються по Ethernet, в кожному кадрі Ethernet переноситься лише один пакет з міткою. Мітка розміщається між заголовком рівня ланки даних і заголовком мережного рівня. Використання MPLS в мережах Ethernet, особливо в міських мережах, є ще однією перспективною можливістю MPLS. До стандарту Ethernet вносяться зміни, що дозволяють збільшити швидкість і дальність передачі Ethernet-пакетів (10 Гбіт/с). На жаль, додавання MPLS-мітки або стека міток до 1492-байтового пакету може привести до необхідності його фрагментації. При передачі пакетів розміру, що віддповідає MTU (Maximum Transmission Unit – максимально можливий розмір передаваного блоку даних) з MPLS-міткою протокол управління передачею TCP визначає, що в MPLS-мережі потрібно провести фрагментацію. Проте слід зазначити, що багато Ethernet-каналів підтримують передачу 1500-байтових або 1508-байтових пакетів.

Отже, мітка може бути розташована в пакеті різними способами – вписується в спеціальний заголовок, що розміщується між заголовками рівня 2 і рівня 3, або у вільному і доступному полі заголовка одного з цих двох рівнів, якщо, звичайно, таке є. Питання про те, куди слід поміщати заголовок, що містить мітку, повинно узгоджуватися між об'єктами, які її використовують.

4.2.3 Комутований по мітках маршрут LSP

Маршрут LSP (Label-Switched Path) є з'єднанням між двома або більш пристроями LSR, в яких для відправки пакетів використовується комутація по мітках, і по якому слідують пакети одного і того ж класу еквівалентності пересилки FEC. Маршрут LSP можна розглядати як шлях через набір LSR-пристроїв, по якому проходять до одержувача пакети, що належать до одного класу FEC.

Маршрути LSP створюються з використанням протоколу LDP, протоколу резервування ресурсів з розширеннями для перерозподілу потоків (Resource Reservation Protocol with Traffic Engineering extensions — RSVP-TE) або за допомогою розширень протоколів маршрутизації, таких як багатопротокольний механізм BGP (Multiprotocol BGP).

Комутація MPLS дозволяє встановити ієрархію міток, відому як стек міток. Внаслідок цього можливе використання різних LSP-маршрутів для різних рівнів міток при відправці пакету до пункту призначення. Такі маршрути створюються лише для передачі пакету в одному напрямі. Дане твердження також означає, що для зворотнього шляху назад може бути використаний інший маршрут.

На рис. 4.9 пристроями LSR1 і LSR6 є граничні LSR-маршрутизатори, а LSR2, LSR3, LSR4 і LSR5 є базовими маршрутизаторами LSR, Для відправки пакетів маршрутизатори LSR1 і LSR6 здійснюють паритетний обмін інформацією на рівні граничних шлюзів, а маршрутизатори LSR2, LSR3, LSR4 і LSR5 – на рівні внутрішніх шлюзів. На рис. 4.9 показано два маршрути LSP:

наскрізний LSP-маршрут 1-го рівня від пристрою LSR1 до LSR6 і LSP-маршрут 2-го рівня між пристроями LSR4 і LSR5.

Набор пакетів, що передається по LSP, відноситься до одного FEC, і кожен маршрутизатор LSR в LSP-тунелі призначає для нього свою мітку. Усередині LSP-тракту може створюватися LSP-тунель. Слід зазначити, що частенько початок і кінець тунелю не збігаються з початком і кінцем LSP-тракту. Як правило, тунель коротший. Інколи потік даних може бути настільки великий, що для нього створюється декілька LSP-тунелів між відправником і одержувачем. У одному LSP може бути створені декілька LSP-тунелів з різними точками прийому і передачі, а в кожному тунелі можуть бути створені LSP-тунелі іншого рівня. У цьому виявляється ієрархічність структури MPLS.

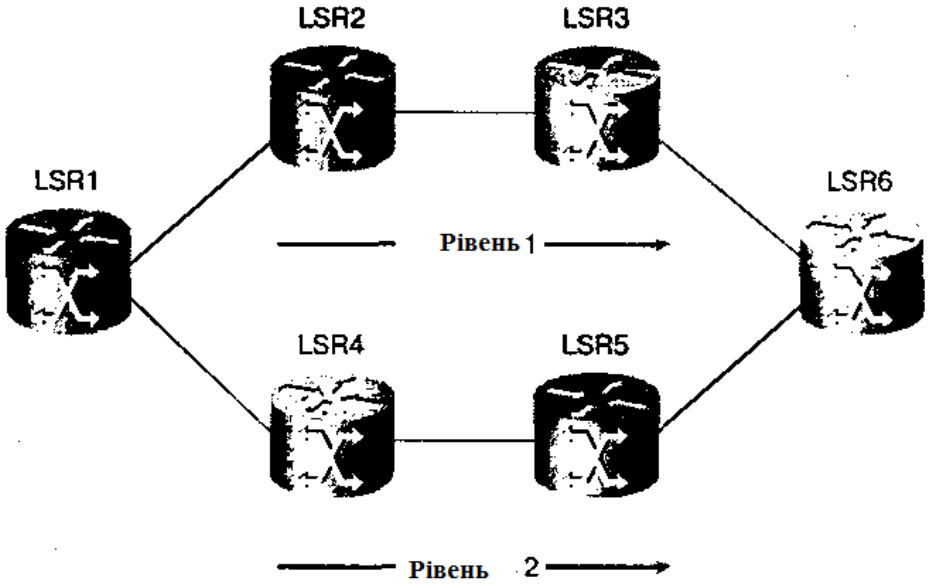


Рис. 4.8 - Рівні маршруту з комутацією по міткам

У мережі MPLS може існувати набір маршрутизаторів, які є вхідними для конкретного FEC, тоді вважається, що для цього FEC існує LSP-тунель з різними точками входу і виходу.

Якщо для деяких з цих LSP вихідним є один і той же LSR, то можна говорити про дерево LSP, коренем якого служить даний вихідний маршрутизатор.

LSP можна розглядати як тракт, що створюється шляхом зчеплення одного і більш ділянок маршруту, який дозволяє пересилати пакет, замінюючи на кожному вузлі мережі MPLS вхідну мітку вихідною міткою (так званий алгоритм перестановки міток). Таким чином, тракт мережі MPLS можна розглядати як тунель, для створення якого в IP-пакет вставляється заголовок – мітка.

LSP встановлюються або перед передачею даних (з управлінням від програми), або при виявленні певного потоку даних (керовані даними LSP).

4.3 Принцип роботи мережі MPLS

Будь-який IP-пакет на вході в мережу MPLS, незалежно від того, поступає цей пакет від відправника або ж він прийшов з суміжної мережі, яка може бути MPLS - мережею більш високого рівня, відноситься до певного класу еквівалентної пересилки FEC (Forwarding Equivalence Class). Нагадаємо, що аналіз заголовка IP-пакета і призначення FEC проводиться лише один раз на вході в мережу (рис.4.9).

Розглянемо алгоритм пересилки по мітці.

Етап 1. Мережа автоматично формує таблиці маршрутизації. У цьому процесі беруть участь маршрутизатори або комутатори IP+ATM, встановлені в мережі сервіс-провайдера. При цьому застосовуються внутрішні протоколи маршрутизації, такі як OSPF або IS-IS.

Етап 2. Протокол розподілу міток (Label Distribution Protocol – LDP) використовує відображену в таблицях топологію маршрутизації для визначення значень міток, вказуючих на сусідні пристрої. В результаті цієї операції формуються маршрути з комутацією по мітках (Label Switched Paths – LSP). Автоматичное привласнення міток MPLS вигідно відрізняє цю технологію від технології приватних віртуальних каналів ATM PVC, що вимагають ручного привласнення VCI/VPI.

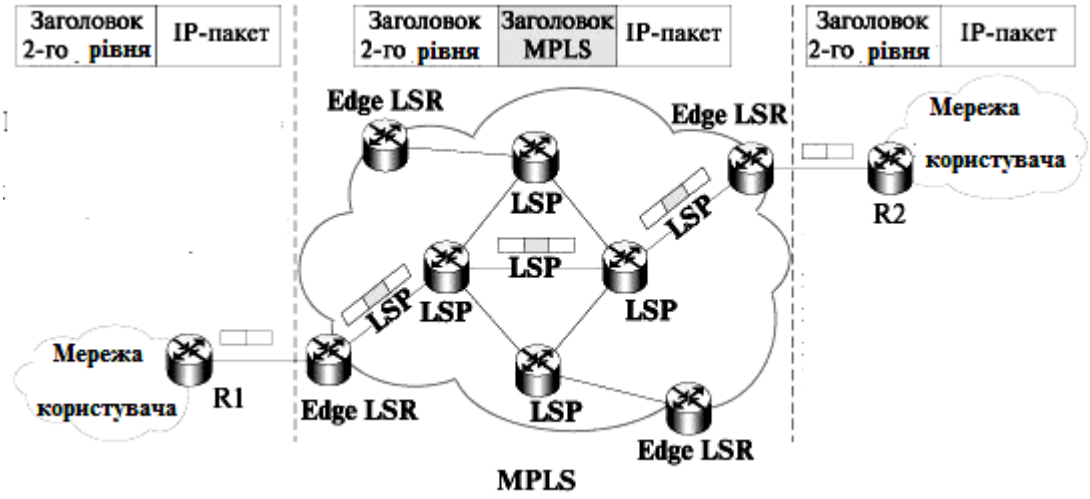


Рис. 4.9 – Фрагмент MPLS - мережі

R1, R2 - граничні маршрутизатори мережі користувача
LSP - комутований по мітках маршрут
LSR- маршрутизатор, що підтримує комутацію по мітках і традиційну IP-маршоутизацію
Edge LSR- граничний маршрутизатор, який підключено до пристроїв,
які не підтримують комутацію по мітках

Етап 3. Вхідний пакет поступає на граничний Label Switch Router (LSR), який визначає, які послуги 3-го рівня необхідні цьому пакету (наприклад QoS або управління смугою пропускання). З врахуванням всіх вимог маршрутизації і правил високого рівня, пограничний LSR вибирає і привласнює мітку, яка записується в заголовок пакету, після чого пакет передається далі.

Етап 4. Пристрій LSR, що знаходиться в опорній мережі, прочитує мітки кожного пакету, замінює старі мітки новими (нові мітки визначаються по локальній таблиці) і передає пакет далі. Ця операція повторюється в кожній точці передачі пакету по опорній мережі.

Етап 5. На виході пакет потрапляє в пограничний LSR, який видаляє мітку, прочитує заголовок пакету і передає його за місцем призначення. У магістральних LSR мітка MPLS порівнюється із заздалегідь розрахованими таблицями комутації і містить інформацію 3-го рівня. Це дозволяє кожному пристрою LSR автоматично надавати кожному пакету необхідні IP-услуги. Таблиці розраховуються заздалегідь, що знімає необхідність повторної обробки пакетів в кожній точці передачі. Така схема не лише дозволяє розділити різні типи трафіку (наприклад, відокремити непріоритетний трафік від критично важливого); вона робить рішення MPLS добре масштабованими. Оскільки для привласнення міток технологія MPLS використовує різні набори правил (policy mechanisms), вона відділяє передачу пакетів від вмісту заголовків IP. Мітки мають лише локальне значення і багато разів використовуються в крупних мережах, тому вичерпати запас міток практично неможливо. В рамках надання корпоративних IP-послуг найголовніша перевага MPLS полягає в здатності привласнювати мітки, що мають спеціальне значення. Набори міток визначають не лише місце призначення, але і тип додатку і клас обслуговування.

4.3.1 Таблиці пересилки пакетів

Кожен вузол мережі MPLS підтримує дві таблиці, за допомогою яких визначає, яким чином повинен пересилатися пакет. Таблиці називаються:

- інформаційна база LIB (Label Information Base);
- інформаційна база пересилки LFIB (Label Forwarding Information Base).

Кожна з них містить використовувану множину міток і для кожної з них є запис, що визначає прив'язку "FEC-мітка". Проте, LIB містить мітки, призначені локальним MPLS-вузлом (шляхом перегляду своєї таблиці маршрутизації і призначення кожному FEC мітки, тобто LIB – містить всі мітки відомі LSR, незалежно від того чи використовується мітка для передачі даних чи ні). LFIB містить мітки, отримані від сусідніх вузлів або з LIB перед відправкою пакету.
Таким чином за допомогою LIB і LFIB забезпечується два типи прив'язки міток до FEC:

- перший тип – мітка для прив'язки вибирається і призначається в LSR локально. Така прив'язка називається локальною (так заповнюється LIB);
- другий тип – LSR отримує від деякого іншого LSR інформацію про прив'язку мітки, яка відповідає прив'язці, створеній на цьому іншому LSR. Така прив'язка називається віддаленою (так заповнюється LFIB).

Для пересилки пакетів використовується LFIB. Ця таблиця (яку веде кожен LSR) є послідовністю записів. Кожен запис таблиці пересилки LSR складається з вхідної мітки і одній або більш вкладених записів, причому кожна такий

підзапис містить значення виходної мітки, ідентифікатор вихідного інтерфейсу і адресу наступного маршрутизатора в маршруті LSP. Фактично значення вхідної мітки є індексом для пошуку в базі LFIB. Декілька вкладених записів необхідно для багатоадресної розсилки, коли пакет, який поступив до одного вхідного інтерфейсу, повинен потім розсилатися через декілька вихідних інтерфейсів. Запис в таблиці може також містити інформацію, вказуючу, 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 обробка пакету визначається виключно міткою, що переноситься в пакеті. У другому варіанті обробка пакету визначається не лише міткою, але і інтерфейсом, на який поступив пакет. LSR може використовувати або перший варіант, або другий, або їх поєднання.

Засоби управління комутацією по мітках використовують для заповнення таблиць пересилки як локальну, так і віддалену прив'язку міток до FEC. Це може робитися в двох варіантах: downstream і upstream.

Перший (downstream): коли мітки на локальній прив'язці використовуються як вхідні мітки, а мітки з віддаленої прив'язки – як вихідні.

Другий варіант (upstream) – прямо протилежний, тобто мітки з локальної прив'язки використовуються як вихідні мітки, а мітки з віддаленої прив'язки – як вхідні. Розглянемо кожен з цих варіантів.

Таблиця 4.2 – Таблиця пересилки LFIB

Вхідна мітка	**Перший підзапис**	**Другий підзапис**
Значення вхідної мітки	Вихідна мітка	Вихідна мітка
	Вихідний інтерфейс	Вихідний інтерфейс
	Адреса наступного LSR	Адреса наступного LSR
Значення вхідної мітки	Вихідна мітка	Вихідна мітка
	Вихідний інтерфейс	Вихідний інтерфейс
	Адреса наступного LSR	Адреса наступного LSR

Перший варіант називається прив'язкою мітки до FEC "знизу" (downstream label binding), тому що в цьому випадку прив'язка мітки, що переноситься пакетом, до того FEC, якому належить цей пакет, створюється нижчестоячим LSR, тобто LSR, розташованим ближче до адресата пакету, чим LSR, який поміщає мітку в пакет. При прив'язці "знизу" пакети, які переносять певну мітку, передаються в напрямі, протилежному до напряму передачі інформації про прив'язку цієї мітки до FEC.

Другий варіант називається прив'язкою мітки до FEC "зверху" (upstream label binding), тому що в цьому випадку прив'язка мітки, що переноситься пакетом, до того FEC, якому належить цей пакет, створюється тим же LSR, який поміщає мітку в пакет; тобто творець прив'язки розташований "вищим" (ближче до відправника пакету), ніж LSR, до якого пересилається цей пакет. При

прив'язці "зверху" пакети, які переносять певну мітку, передаються в тому ж напрямі, що і інформація про прив'язку цієї мітки до FEC.

LSR обслуговує також пул "вільних" міток (тобто міток без прив'язки). При початковій установці LSR пул містить всі мітки, які може використовувати LSR для їх локальної прив'язки до FEC. Саме ємність цього пулу і визначає, кінець кінцем, скільки пар "мітка - FEC " може одночасно підтримувати LSR. Коли маршрутизатор створює нову локальну прив'язку, він бере мітку з пулу; коли маршрутизатор знищує раніше створену прив'язку, він повертає мітку, пов'язану з цією прив'язкою, назад в пул.

4.3.2 Створення маршрутів LSP

Маршрути LSP можуть бути встановлені одним з таких способів:

- шляхом використання механізму незалежного контролю;
- шляхом використання механізму впорядкованого контролю.

Незалежний і впорядкований контроль для встановлення LSP-маршрутів можуть співіснувати в одній і тій же мережі; при цьому не виникають структурні проблеми або проблеми взаємодії. Незалежний метод забезпечує швидшу збіжність і установку маршрутів LSP, оскільки LSR-пристрої можуть встановлювати і анонсувати прив'язку міток у будь-який момент, не витрачаючи час на поширення повідомлень від однієї межі мережі до іншої. Установка маршруту LSP відбувається відразу ж після завершення конвергенції протоколів маршрутизації.

Примітка. *Конвергенцією називається процес встановлення домовленості між всіма маршрутизаторами про наявні маршрути. В результаті конвергенції всі маршрутизатори в мережі володіють однаковою інформацією про її структуру і маршрути.*

При використанні методу впорядкованого контролю перед установкою маршруту LSP відбувається поширення інформації про прив'язку міток. Проте такий метод контролю надає великі можливості запобігання в мережі кільцевих маршрутів.

4.3.2.1 Встановлення LSP-маршрутів методом незалежного контролю

При установленні маршрутів LSP методом незалежного контролю кожний LSR-пристрій розподіляє свої префікси одержувачів між класами FEC. Кожному класу FEC призначається мітка, і всі сусіди LSR-пристрою оповіщаються про прив'язку міток. Всі сусідні LSR-пристрої створюють бази LFIB, використовуючи перетворення класів FEC в адреси наступних транзитних переходів. Для перетворення класу FEC на адресу наступної точки переходу LSR-пристрої зазвичай використовують протоколи маршрутизації, засновані на одноадресній розсилці, такі як OSPF або IS- IS.

База LFIB містить дані наступних полів: вхідної мітки, вихідний мітки, адреса наступного транзитного переходу і вихідного інтерфейсу. LSR-пристрій

створює локальний запис прив'язки конкретного FEC-класу, довільним чином вибираючи мітку з пулу (тобто набору) вільних в даний момент (вакантних) міток в інформаційній базі міток (Label Information Base - LIB), і оновлює свою базу LFIB. Поле вхідної (incoming) мітки в базі LFIB встановлюється рівним значенню мітки, вибраної з пулу. Адрес наступного переходу встановлюється рівним адресу наступного транзитного пристрою 3-го рівня, пов'язаного з даним класом FEC, а поле вихідного інтерфейсу (outgoing interface) встановлюється рівним номеру вихідного інтерфейсу, використовуваного для наступного транзитного переходу.

Після створення локальної таблиці LSR-пристрій повідомляє інформацію про локальну відповідність міток сусіднім LSR- пристроям, використовуючи протокол LDP або розширення модифікованого протоколу маршрутизації. Поширювана інформація про прив'язку міток складається з набору кортежів (групи взаємозв'язаних записів), що складаються з префікса адреса (address prefix) і мітки (label), де префікс адреса вказує клас FEC (в разі простої маршрутизації з одноадресною розсилкою), а параметр label задає значення мітки, яке LSR-пристрій використовує для побудови локальної таблиці зв'язків міток з конкретним класом FEC.

Коли LSR-пристрій отримує інформацію про мітку від свого сусіда, він перевіряє наявність локального запису про прив'язку мітки в своїй базі LFIB. Якщо локальний запис є, то значення вихідний мітки (outgoing label) для цієї позиції оновлюється і замінюється тільки що набутим значенням. З цієї миті LSR-пристрій має повністю заповнену позицію в базі LFIB і готовий до відправки пакетів. Якщо LSR-пристрій отримує інформацію про мітки від сусіднього пристрою, але не має в своїй базі LFIB локального запису для даного класу FEC, то у нього є можливість зберегти цю інформацію (вона може згодитися пізніше) або відкинути її. Якщо інформація відкидається, то протокол LDP запрошує в сусіднього пристрою відомості про мітку. Інформація про прив'язку міток поширюється лише між суміжними LSR- пристроями. Будь-який LSR-пристрій спільно використовує інформацію про мітки лише з сусіднім LSR-пристроєм, який спільно використовує єдину підмережу принаймні з одним інтерфейсом локального LSR- пристрою.

Розглянемо алгоритм установки маршруту на конкретному прикладі (рис.4.10). Як показано на рисунку, префікс адреси 172.160.0/16 безпосередньо пов'язаний з пристроєм LSR6. Пристрої LSR3 і LSR5 використовують маршрутизатор LSR6 як вузол наступного транзитного переходу для класу FEC 172.16.0.0/16.

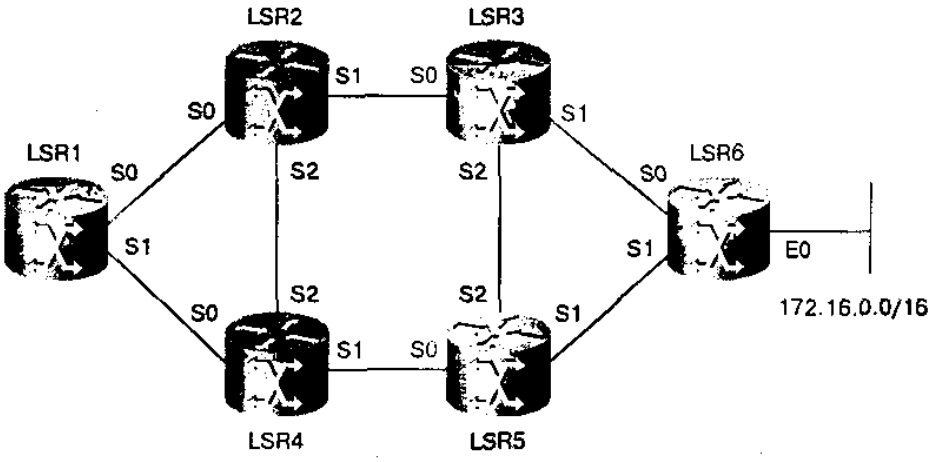


Рис. 4.10 – Встановлення маршруту LSP методом незалежного контролю

1) Пристрій LSR1 визначає, чи відповідає адрес наступного переходу для класу FEC маршрутизатору LSR2, який пов'язаний з класом 172.16.0.0/16 за допомогою протоколу одноадресної розсилки, такого, наприклад, як OSPF. Після цього пристрій LSR1 довільно вибирає мітку зі свого пулу міток, використовуючи свою базу LIB. Припустимо, що значення відповідної мітки дорівнює 50. Пристрій LSR1 використовує мітку як індекс своєї бази LFIB для знаходження відповідної позиції, яка оновлюватиметься. Після того, як виявлена відповідність, значення вхідної мітки (incoming label) в цій позиції встановлюється рівним 50. Як наступний перехід (next hop) встановлюється пристрій LSR2, а як вихідний інтерфейс (outgoing interface) вибирається інтерфейс S0. На цьому етапі значення вихідний мітки (outgoing label) не встановлюється.

2) Пристрій LSR1 посилає інформацію про локальну прив'язку міток пристроям LSR2 і LSR4.

3) У цей момент ні маршрутизатор LSR2, ні маршрутизатор LSR4 не використовують пристрій LSR1 як вузол наступного переходу для досягнення мережі 172.16.0.0/16, тому вони не можуть відновити свої вихідні мітки в базах LFIB для класу FEC 172.16.0.0/16.

4) LSR2 довільно вибирає мітку зі свого пулу, використовуючи власну базу LIB. Припустимо, що значення мітки, довільно вибране пристроєм LSR2, дорівнює 25. Пристрій LSR2 використовує мітку як індекс своєї бази LFIB для пошуку співпадаючої позиції, яка буде оновлена. Після того, як відповідність знайдена, вхідна мітка (incoming label) в записі встановлюється рівною 25. LSR2 посилає інформацію про свої локальні мітки пристроям LSR1, LSR3 і LSR4.

5) LSR3 не використовує пристрій LSR2 як вузол наступного переходу для досягнення мережі 172.16.0.0/16, тому не оновлює свої вихідні мітки в базах LFIB для класу FEC 172.16.0.0/16. Перипустимо, що значення локальної мітки, довільно вибране пристроєм LSR3, дорівнює 45. LSR3 посилає інформацію про свої локальні мітки пристроям LSR2, LSR5 і LSR6.

6) Пристрій LSR1 отримує інформацію від маршрутизатора LSR2 про його локальні мітки. Оскільки пристрою LSR1 відомо, що інформація поступила від сусіднього вузла, який є наступним транзитним переходом для мережі 172.16.0.0/16, то LSR1 використовує її як інформацію віддаленого пристрою для цього запису, тобто LSRI використовує мітку, надану пристроєм LSR2 для оновлення вихідний мітки (outgoing label) в записі своєї бази LFIB, яка пов'язана з класом FEC 172.16.0.0/16. Якщо пристрій LSR1 виконує функцію вхідного граничного пристрою для такого маршруту LSP, то він не задає значення вхідної мітки.

7) Пристрій LSR2 отримує інформацію від маршрутизатора LSR3 про його локальні мітки. Оскільки пристрою LSR2 відомо, що інформація поступила від сусіднього вузла, який є наступним транзитним переходом для мережі 172.16.0.0/16, то LSR2 використовує її як інформацію віддаленого пристрою для цього запису, тобто LSR2 використовує мітку, надану пристроєм LSR3 для оновлення вихідної мітки (outgoing label) в записі своєї бази LFIB, яка пов'язана з класом FEC 172.16.0.0/16.

8) Аналогічним чином пристрій LSR4 визначає, що маршрутизатор LSR5 є наступним транзитним переходом для класу FEC, пов'язаного з мережею 172.16.0.0/16. Тепер пристрій LSR4 довільним чином вибирає мітку зі свого пулу, використовуючи базу LIB. Припустимо, що значення цієї мітки дорівнює 65. Після цього пристрій LSR4 використовує цю мітку як індекс в своє базі LFIB для знаходження співпадаючої позиції, яка буде змінена. Після того, як знайдена відповідність, поле вхідної мітки (incoming label) даної позиції встановлюється рівним 65. Як наступний транзитний перехід (next hop) встановлюється маршрутизатор LSR5, а як вихідний інтерфейс (outgoing interface) використовується порт S1. Потім пристрій LSR4 посилає інформацію про локальну таблицю міток пристроям LSR1, LSR2 і LSR5. У цей момент жодний з пристроїв LSR1, LSR2, LSR5 не використовує маршрутизатор LSR2 як наступний транзитний перехід до мережі 172.16.0.0/16 і, отже, не може відновити вихідну мітку в записі бази LFIB для мережі 172.16.0.0/16.

9) Проте, коли маршрутизатор LSR5 посилає локальну інформацію пристроям LSR4, LSR3 і LSR6, пристрою LSR4 відомо, що інформація поступила від маршрутизатора наступного транзитного переходу для мережі 172.16.0.0/16 і він використовує цю інформацію як таблицю міток віддаленого пристрою для класу 172.16.0.0/16. Припустимо, що таке довільно вибране пристроєм LSR5 значення мітки дорівнює 95. Після цього пристрій LSR4 використовує мітку, надану пристроєм LSR5, для оновлення своєї вихідної мітки (outgoing label) в запису бази LFIB, пов'язаною з класом FEC 172.16.0.0/16.

10) Коли маршрутизатор LSR6 посилає свою інформацію про локальні мітки пристроям LSR3 і LSR5, цим пристроям відомо, що вона поступила від вузла наступного транзитного переходу для мережі 172.16.0.0/16, і вони обидва використовують її як таблицю міток віддаленого пристрою для класу FEC 172.16.0.0/16. Припустимо, що це довільно вибране пристроєм LSR5 значення мітки дорівнює 33. В такому разі обидва пристрої, LSR3 і LSR5, використовують

мітку, надану пристроєм LSR6, для обновлення вихідній мітки (outgoing label) в записах своїх баз LFIB, пов'язаних з класом FEC 172.16.0.0/16. Пристрій LSR6 не містить вихідний мітки в базі LFIB для класу 172.16.0.0/16, оскільки він безпосередньо приєднаний до мережі 172.16.0.0/16. Для цієї мережі пристрій LSR6 є граничним LSR-пристроєм, тому він видаляє мітку з пакету перед відправкою його в мережу 172.16.0.0/16.

Таблиця 4.3 – Записи бази LFIB після розповсюдження міток

Пристрій	Вхідна мітка	Вихідна мітка	Наступний транзитний перехід	Вихідний інтерфейс
LSR1	50	25	LSR2	S0
LSR2	25	45	LSR3	S1
LSR3	45	33	LSR6	S1
LSR4	65	95	LSR5	S1
LSR5	95	33	LSR6	S1
LSR6	33	-	LSR6	E0

На цій стадії, як показано в таблиці 4.3, у всіх LSR-пристроїв записи баз LFIB для класу FEC 172.16.0.0/16 заповнені, і вони готові до пересилки пакетів. Коли пристрій LSR1 отримує пакет із значенням мітки, рівним 50, він використовує її як індекс своєї інформаційної бази LFIB для пошуку запису необхідного для пересилки пакетів. Після того, як відповідна позиція знайдена, пристрій обмінює значення мітки на значення вихідний мітки, рівної 25, і відправляє пакет через інтерфейс S0 на пристрій LSR2, який здійснює аналогічний пошук по своїй базі, обмінює значення мітки на значення 45 і направляє пакет пристрою LSR3 через інтерфейс S1. Пристрій LSR3 виконує пошук в базі LFIB, міняє значення мітки на 33 і направляє пакет пристрою LSR6 через інтерфейс S1. Зрештою пристрій LSR6 видаляє мітку з пакету і направляє його до пункту призначення через інтерфейс E0. В разі видалення мітки на передостанньому переході, тобто на пристрої LSR3, маршрутизатор LSR6 може виконати пошук або в базі LFIB, або в таблиці маршрутизації 3-го рівня.

4.3.2.2 Встановлення маршруту LSP за допомогою механізму впорядкованого контролю

При використанні для встановлення маршруту LSP методу впорядкованого контролю вхідний або вихідний граничний LSR-пристрій ініціює установку маршруту LSR. Призначення міток відбувається впорядкованим чином від кінцевої (вихідний) до початкової (вхідний) точок LSP-маршруту. Установка дороги LSP може бути почата з будь-якого кінця – з входу або з виходу. Пристрій, що ініціює створення маршруту LSP, вибирає класи FEC, і всі останні LSR- пристрої на даному LSP-маршруті

використовують ті ж самі записи FEC. Такий метод контролю при установці маршруту LSP вимагає, аби інформація про прив'язку міток була розповсюджена по всіх LSR-пристроях до визначення маршруту LSP. Описуваний підхід наводить до того, що час конвергенції при цьому у декілька разів більше, ніж при незалежному контролі. Проте при використанні методу впорядкованого контролю імовірність виникнення петель на маршруті LSP менше ніж при незалежному контролі.

Приклад встановлення LSP-маршруту впорядкованим методом наведений на рис. 4.11. В даному прикладі пристрій LSR7 є вихідним LSR-маршрутизатором, який ініціює установку LSP-маршруту.

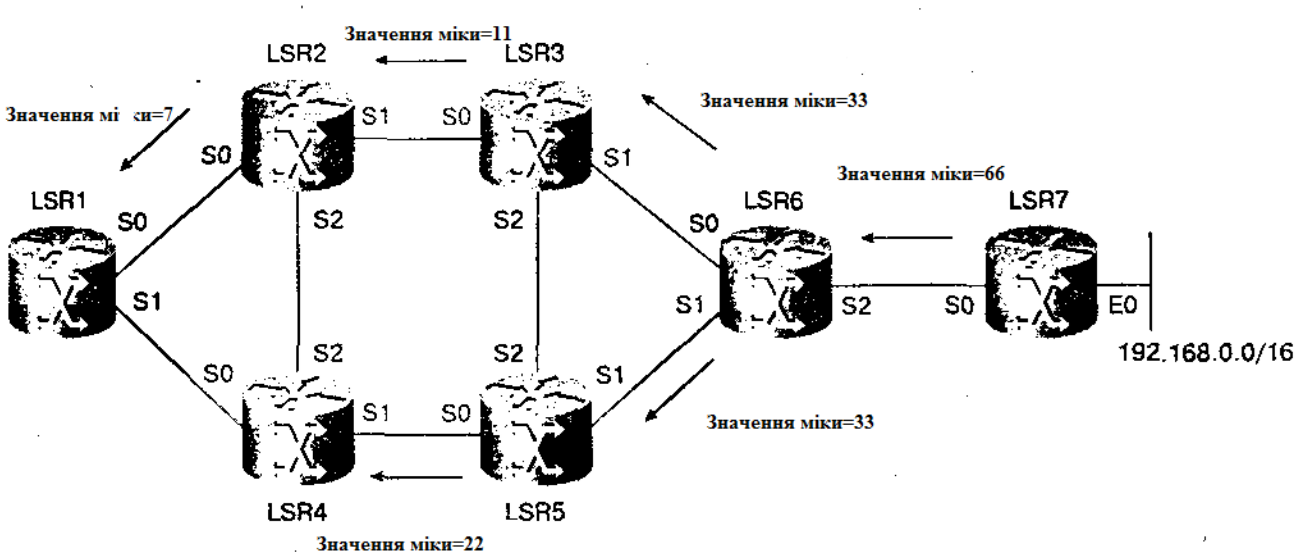


Рис. 4.11 – Встановлення маршруту LSP методом впорядкованого контролю

Пристрій LSR7 має безпосереднє з'єднання з мережею 192.168.0.0/16. Припустимо, що маршрутизатор LSR7 призначає класу FEC 192.168.0.0/16 мітку із значенням 66. Після цього він сповіщає про свою локальну мітку сусідній пристрій LSR6. Отримавши таке сповіщення, маршрутизатор LSR6 призначає даному класу FEC нову мітку із значенням 33 і повідомляє про прив'язку мітки до мережі своїм сусідам: пристроям LSR3 і LSR5. Впорядкована установка маршруту LSP продовжується в такий спосіб впродовж всього маршруту LSP до вхідного пристрою LSR1.

Архітектура MPLS не передбачає вживання якогось єдиного протоколу розподілу міток. У одній і тій же мережі MPLS можуть використовуватися:

- спеціальний протокол розподілу міток Label Distribution Protocol (LDP);
- протокол сигналізації RSVP;
- розширення можливостей протоколів маршрутизації, наприклад протоколу междоменної маршрутизації Border Gateway Protocol (BGP).

4.4 Принцип роботи маршрутизатора LSR в мережі MPLS

LSR (Label-Switched Router) є пристроєм, що виконує функції управління і відправки при використанні MPLS-комутації. LSR-пристрій пересилає пакет, грунтуючись на значенні мітки, інкапсульованому в пакеті.

Маршрутизатор LSR може також пересилати звичайні пакети третього рівня. В якості LSR-пристроїв можуть виступати маршрутизатори, виконуючі MPLS-комутацію, або ATM-коммутаторы, що мають функції MPLS і використовують мітки для відправки даних. Пакетні LSR-пристрої легко можуть бути створені шляхом завантаження образу IOS з набором функцій MPLS на звичайний маршрутизатор. LSR-пристрої MPLS в мережі ATM можуть бути створені за допомогою комутатора ATM з інтегрованим програмним забезпеченням MPLS або шляхом додавання функцій MPLS з використанням зовнішнього контролера LSC.

Фундаментальною основою комутації по мітках є те, що LSR- пристрої погоджують свої дії відносно міток, використовуваних для передачі даних. Таке узгодження здійснюється шляхом використання протоколу розповсюдження міток або розширень протоколів PIM, BGP, RSVP або CR-LDP.

Граничні LSR-пристрої знаходяться в точках присутності провайдерів (Point of Presence - PoP) на межах мережі MPLS і призначають пакетам мітки (або стеки міток). Прив'язка міток або впровадження їх в початок пакету також називаються "вставкою" (push) міток. Граничні пристрої LSR вставляють або видаляють мітки в точці виходу пакетів з MPLS-домена, що називається "витісненням" (pop) мітки. Граничні LSR-пристрої можуть також виконувати звичайні функції пересилки пакетів по протоколу IP.

Дії, які можуть виконувати LSR- пристрої над поміченими пакетами:

- Агрегація – видаляє верхню мітку стека і виконує пошук інформації 3-го рівня.
- Витіснення – видаляє верхню мітку стека і передає корисне навантаження пакету у вигляді IP-пакета з міткою або без неї.
- Вставка – замінює верхню мітку стека набором міток.
- Заміна – замінює верхню мітку стека іншим значенням.
- Видалення тега – видаляє верхню мітку і направляє IP-пакет за вказаною адресою наступного IP-перехода.

Розглянемо принцип роботи пакетних LSR-пристроїв.

Для передачі пакетів третього рівня по мережі, що працює на основі маршрутизаторів, пакетна технологія MPLS використовує принцип передачі пакетів по мітках. Основні функції пакетного середовища MPLS по підтримці одноадресної маршрутизації з однорівневим стеком міток показані на рис. 4.12. Пристрій LSR1 виконує функції граничного маршрутизатора LSR. Він привласнює пакету первинну мітку після застосування алгоритму найбільшої відповідності до заголовка IP і призначення пакету класу FEC. В разі використання технології VPN на вибір класу FEC можуть також впливати такі параметри, як номер вхідного інтерфейсу або заздалегідь задане правило

перерозподілу потоків. Призначення пакету класу FEC відбувається лише один раз – під час вступу пакету в мережу.

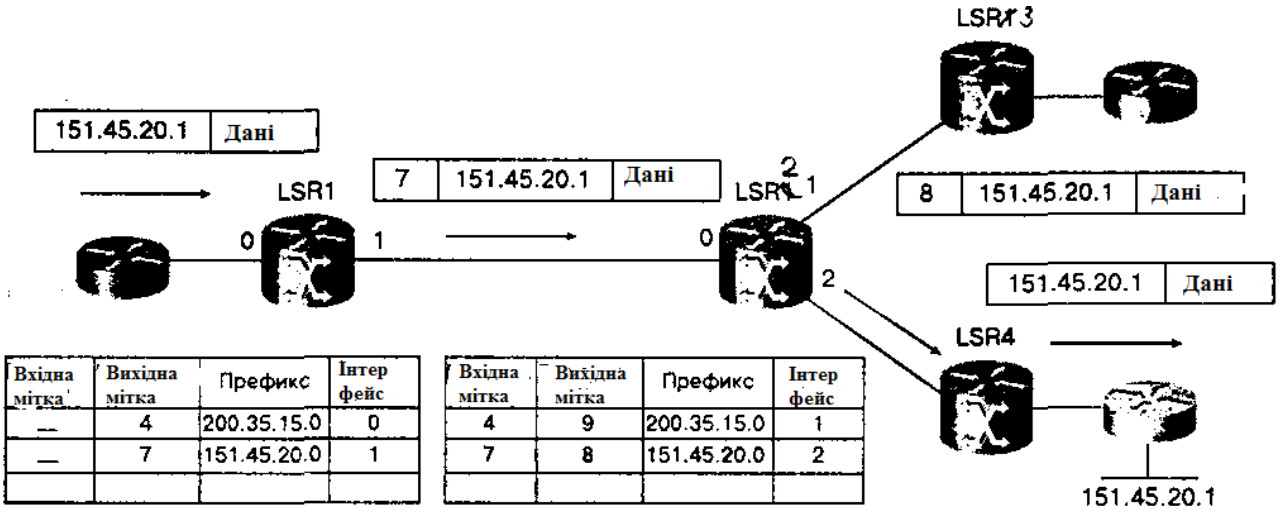


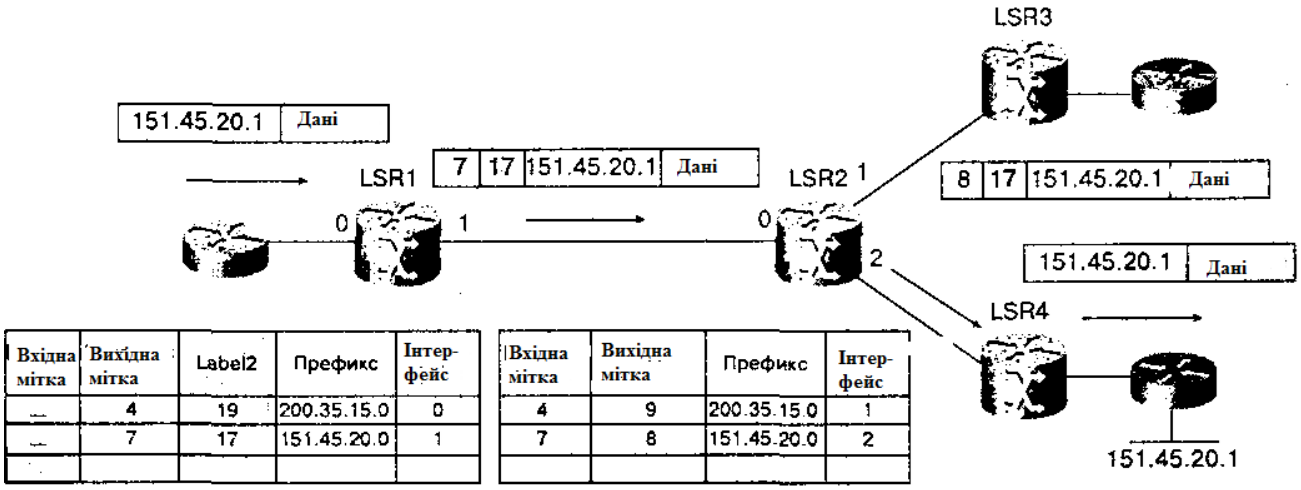
Рис. 4.12 – Функції LSR-пристроїв для однорівневого стека міток

Кожному класу FEC відповідає певна мітка. Після того, як пакету привласнено мітку, наступні LSR-пристрої направляють його далі, використовуючи лише цю мітку. LSR-пристрій зазвичай замінює мітку на вхідному пакеті новим значенням в той момент, коли передає цей пакет далі. На виході з мережі пристрій LSR4 переглядає мітку, видаляє її, виконує аналіз інформації 3-го рівня і направляє пакет на зовнішній маршрутизатор наступного транзитного переходу. На рис. 4.13 показані операції LSR-пристроїв з пакетами за наявності в стеку де кількох рівнів міток.

Пристрій LSR1 виконує функції граничного маршрутизатора LSR. Він призначає пакету первинний набір міток після застосування звичайного алгоритму найбільшої відповідності до IP-заголовку і визначає для пакету клас FEC. Проміжний пристрій LSR2 видаляє верхню мітку стека "7" і замінює її міткою із значенням "8". На виході з мережі пристрій LSR4 переглядає мітки, видаляє мітку, аналізує інформацію третього рівня і направляє пакет на зовнішній маршрутизатор наступного транзитного переходу.

Розглянемо особливості функціонування LSR-пристроїв мережі ATM. При комутації MPLS в середовищі ATM використовується метод пересилки на основі міток для передачі пакетів 3-го рівня у вигляді ATM-чарунок по базовій мережі ATM. Комутація MPLS в мережах ATM також називається режимом передачі чарунок MPLS. LSR-пристрій середовища ATM є ATM-комутатор, що має функції MPLS. LSR-пристрої мережі ATM зазвичай мають контролер LSC, який разом з іншими LSR-пристроями виконує функції IP-маршрутизации в мережі MPLS. Комутований по мітках ATM-інтерфейс (label-switching-controlled ATM – LC-ATM) контролюється компонентой управління комутації по мітках. Якщо пакет пройшов через такий інтерфейс, то при отриманні він розглядається як той, що містить мітку. Верхня мітка пакету витягується або з вмісту поля VCI, або з об'єднаного вмісту полів VPI і VCI. LSR-пристрій ATM є маршрутизатором LSR з декількома інтерфейсами LC-ATM. Пристрої LSR

мережі ATM направляють чарунки на ці інтерфейси, використовуючи мітки, що містяться в полі VCI або в полі VPI/VCI без повторної збірки чарунок у фрейми перед відправкою. LSR-пристрої середовища ATM використовують управляючи протоколи MPLS в площині управління і встановлюють віртуальні канали з комутацією по мітках (Label Virtual Circuits – LVC), які є MPLS-аналогом звичайних PVC- каналів мережі ATM. Пакети з мітками відправляють як чарунки ATM. Матриця комутації комутатора ATM використовується як інформаційна база пересилки даних по мітках.



Вхідна мітка	Вихідна мітка	Label2	Префикс	Інтер-фейс
—	4	19	200.35.15.0	0
—	7	17	151.45.20.0	1

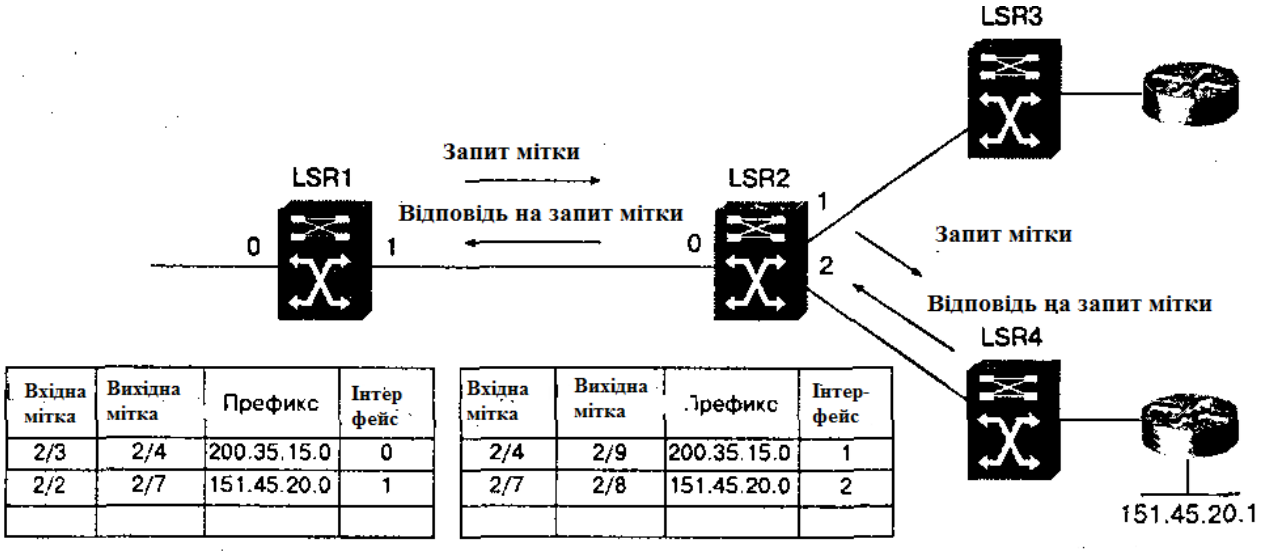
Вхідна мітка	Вихідна мітка	Префикс	Інтер-фейс
4	9	200.35.15.0	1
7	8	151.45.20.0	2

Рис. 4.13 – Функції LSR-пристроїв для багаторівневого стека міток

Граничний LSR-пристрій середовища ATM отримує помічені або непомічені пакети, сегментує їх у чарунки ATM і направляє ці чарунки на наступний транзитний LSR-пристрій мережі ATM. Граничний LSR-пристрій мережі ATM, що обробляє пакети, зазвичай має принаймні один інтерфейс LC-ATM.

Як показано на рис. 4.14, LSR-пристрої ATM при створенні LSP-маршруту (маршрут з комутацією по мітках) використовують метод впорядкованого контролю (ordered control), оскільки призначення міток здійснюється послідовно (по порядку) від вихідний до вхідної точки LSP-маршруту. Метод розподілу міток, використовуваний протоколом LDP, називається низхідним призначенням за вимогою (downstream on demand), оскільки LSR-пристрої ATM призначають мітки по запиту сусіднього пристрою, що знаходиться вище по маршруту. Якщо LSR-пристрій ATM, що знаходиться нижче по маршруту, не має мітки, яку він міг би використовувати для відповіді на запит про мітку від вищестоячого сусіда, то він запрошує мітку від сусіда, що стоїть нижче. Останній зможе відповісти на запит лише після отримання мітки від LSR-пристрою, що розташовується нижче за нього по маршруту.

Механізм пересилки, використовуваний LSR-пристроями MPLS-комутації в мережах ATM, є звичайною ATM- комутацією чарунок на основі значень VPI/VCI, що містяться в заголовках чарунок. Проте ці значення ідентифікаторів VP1/VCI насправді є мітками. Заголовок стека MPLS LSR- пристроями середовища ATM не використовується, а верхня мітка стека встановлюється рівною 0 вхідним граничним LSR-пристроєм ATM.



Вхідна мітка	Вихідна мітка	Префикс	Інтер фейс
2/3	2/4	200.35.15.0	0
2/2	2/7	151.45.20.0	1

Вхідна мітка	Вихідна мітка	Префикс	Інтер-фейс
2/4	2/9	200.35.15.0	1
2/7	2/8	151.45.20.0	2

Рис. 4.14 – Функціонування LSR-пристроїв мережі ATM

Процедура виділення і призначення мітки в мережі ATM з MPLS-комутацією (рис.4.14) може бути представлена у вигляді наступних етапів:

Етап 1. Пристрій LSRI мережі ATM запрошує мітку для класу FEC 151.45-20.0, використовуючи запит на перетворення мітки протоколу LDP або TDP від розташованого нижче по маршруту сусіднього пристрою LSR2.

Етап 2. Пристрій LSR2, у свою чергу, запрошує мітку для класу FEC 151.45.20.0 від розташованого нижче сусіднього пристрою LSR4, використовуючи запит на перетворення мітки LDP (або TDP для Cisco).

Етап 3. Вихідний пристрій LSR4 виділяє мітку класу FEC 151.45.20.0, який відповідає вхідному значенню пари VPI/VCI, змінює позицію в своїй інформаційній базі LFIB, відповідну даному FEC, і посилає це значення поля VPI/VCI пристрою LSR2, використовуючи відповідь протоколу LDP.

Етап 4. Пристрій LSR2 використовує отримане від пристрою LSR4 значення VPI/VCI як вихідне значення VPI/VCI, виділяє вільний VC-канал, що перетворюється в локальну вхідну пару VPI/VCI, і змінює позицію в своїй базі LFIB, відповідну даному класу FEC. Після цього пристрій LSR2 посилає це значення VPI/VCI пристрою LSR1, використовуючи відповідь TDP/LDP.

Етап 5. Пристрій LSR1 використовує отримане від пристрою LSR2 значення VP1/VCI як вихідне значення VPI/VCI і змінює позицію в своїй базі LFIB, відповідну даному класу FEC.

4.5 Протоколи розподілу міток

Для розподілу міток можуть використовуватися різні методи:

- метод на основі топології (topology-based method): використовує стандартну обробку протоколів маршрутизації (наприклад OSPF і BGP, що розглядаються нижче);
- метод на основі запитів (request-based method): використовує обробку управляючого протоколу на основі запитів (наприклад, протоколу RSVP);
- метод на основі трафіку (traffic-based method): запускає процедуру привласнення і розподілу міток при отриманні пакету.

У всіх цих випадках архітектурою MPLS передбачається, що призначення мітки, тобто її прив'язку до певного FEC, проводить LSR, який є вихідним пограничним маршрутизатором для пакетів цього FEC (рис. 4.15).

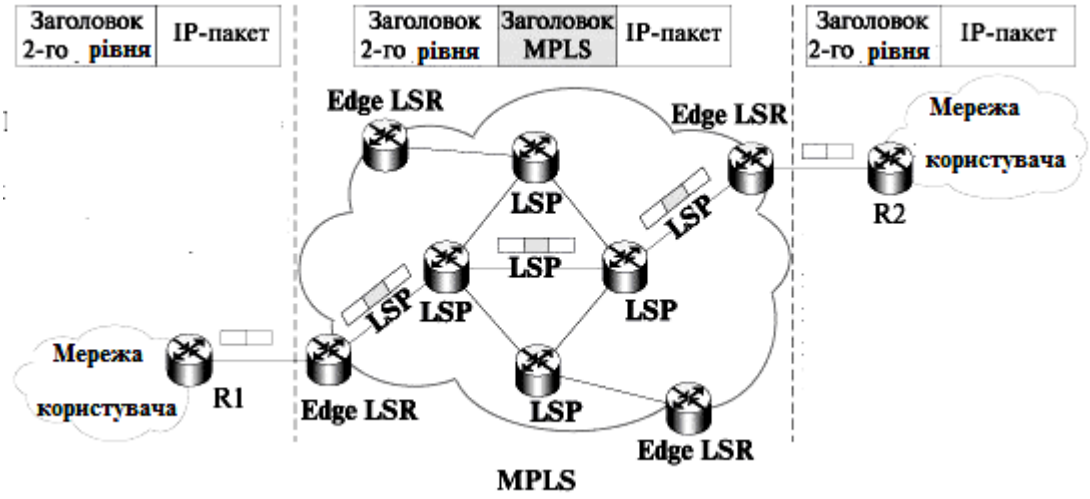


Рис. 4.15 – Фрагмент MPLS-мережі

Таким чином, призначення міток завжди проводиться знизу, тобто в бік, протилежний до напряму трафіка. Нижній LSR інформує сусідні верхні LSR про те, які мітки він прив'язав до кожного FEC пакетів, що поступають до нього. Цей процес і називається розподілом міток, а забезпечує його протокол розподілу міток.

4.5.1 Протокол LDP

Специфікація протоколу LDP визначає правила, за якими встановлюється відповідність між вхідним пакетом і його LSR [22].

Вирішення про призначення міток можуть ґрунтуватися на критеріях пересилки, таких як:

- одноадресна маршрутизація до одержувача;

- оптимізація розподілу трафіку в мережі;
- багатоадресна розсилка;
- віртуальна приватна мережа VPN;
- механізми забезпечення якості обслуговування QoS і ін.

Протокол розподілу міток LDP є набором процедур і повідомлень, за допомогою яких LSR організовує тракти комутації по мітках, обмінюючись інформацією про прив'язку міток в FEC з сусідніми LSR, підтримує і припиняє LSP-сеанси (двосторонній діалог взаємодіючих LSR, що є у даному контексті одноранговими вузлами LDP, в ході якого кожен з взаємодіючих LSR отримує інформацію про прив'язку міток до FEC в іншому LSR).

Процедури протоколу LDP дозволяють LSR, що виконує цей протокол, створювати тракти LSP. Кінцевою точкою такого тракту є або суміжний LSR, що має прямий зв'язок з даним LSR, або вихідний LSR, доступний цьому LSR через деяку кількість транзитних LSR. Процеси виявлення кінцевих точок цих двох типів називаються відповідно процесом базового виявлення і процесом розширеного виявлення. LDP створює двосторонній зв'язок двох суміжних LSR, які стають одноранговими вузлами LDP, що взаємодіють один з одним за допомогою LDP -сеансу.

При обміні між LSR інформацією, пов'язаною з прив'язкою "метка- FEC", використовуються чотири категорії повідомлень LDP:

- повідомлення виявлення (discovery messages), використовувані для того, щоб оголосити і підтримувати присутність LSR в мережі (багатоадресна розсилка "HELLO");
- сеансові повідомлення (session messages), призначені для створення, підтримки і припинення LDP -сеансів між LSR;
- повідомлення-оголошення (advertisement messages), використовувані для створення, зміни і відміни прив'язки мітки до FEC ;
- сповіщаючі повідомлення (notification messages), що містять допоміжну інформацію і інформацію про помилки.

Хоча "роздає" мітки завжди нижній LSR, ініціатором їх розподілу не обов'язково має бути він; процес може ініціювати і верхній LSR, направивши до нижнього LSR відповідний запит; такий режим називається downstream on-demand. У тій або іншій мережі може використовуватися розподіл міток або лише по запитах зверху, або лише за ініціативою нижнього LSR (unsolicited downstream), або і те і інше разом.

Розподіл міток може бути незалежним або впорядкованим. У першому випадку LSR може повідомити вищестоящий LSR про прив'язку мітки до FEC до того, як отримає інформацію про прив'язку від нижчестоящого LSR. У другому випадку висилати подібне повідомлення "вгору" вирішується лише після отримання таких відомостей "знизу".

Нижній LSR розподіляє мітки не лише по тих верхніх LSR, які мають з ним прямі зв'язки. Протокол розподілу міток може бути використаний і для діалогу двох LSR, між якими існує лише комутований зв'язок, проте результат

розподілу в цьому випадку залежить від того, в якому з двох режимів, ліберальному або консервативному, працює верхній LSR.

Режими функціонування протоколу LDP:

- Консервативний режим розподілу міток – в цьому режимі повідомлення-оголошення про прив'язку "мітка - FEC ", отримувані від несуміжних LSR, не приймаються і відкидаються. LSR прив'язує мітку до FEC лише в тому випадку, якщо він є вихідним маршрутизатором або якщо він отримав повідомлення про прив'язку від суміжного з ним LSR. Такий режим дозволяє LSR обслуговувати менше число міток.

- Ліберальний режим розподілу міток – в цьому режимі прив'язка мітки, видана тим нижнім LSR, з яким немає прямого зв'язку, запам'ятовується і використовується. Такий режим зручний тим, що при реконфігурації мережі відповідність між міткою і FEC зберігається, навіть якщо зв'язок з LSR, що визначив це відповідність, став не комутованим, а прямим. Недолік ліберального режиму полягає в тому, що у верхньому LSR доводиться зберігати і обробляти помітно більше інформації про відповідність між мітками і FEC.

Мітка завжди локальна, тобто позначає деякий FEC лише для пари маршрутизаторів, між якими є прямий або комутований зв'язок, і використовується при пересилці пакетів цього FEC від того з маршрутизаторів даної пари, який є в ній верхнім (upstream LSR), до того, який є нижнім (downstream LSR). Для пересилки пакетів того ж FEC до наступного маршрутизатора використовується інша мітка, що ідентифікує цей FEC для нової пари маршрутизаторів, в якій маршрутизатор, що був в попередній парі нижнім, набуває статусу верхнього, а статус нижнього отримує другий маршрутизатор цієї нової пари. Звідси ясно, що кожен маршрутизатор MPLS-мережі повинен зберігати відповідність між вхідними і вихідними мітками для всіх FEC, якими він оперує.

4.5.2 Протокол RSVP для MPLS

Функції, які може виконувати RSVP в мережі MPLS:

- розподіл міток (замість протоколу LDP).
- підтримка QoS в мережі MPLS (незалежно від використовуваного протоколу розподілу міток, маршрутизатори LSR повинні погоджувати між собою параметри QoS для кожного FEC. Мітки дозволяють визначити величезне число класів QoS, але реально в типових мультисервісних мережах, навіть при дуже великій кількості класів FEC, існуватимуть, як правило, всього декілька класів QoS).

Мета введення в мережу MPLS функцій підтримки протоколу RSVP полягає в тому, аби LSR могли розпізнавати пакети, що належать тим потокам, для яких було зроблено резервування ресурсів. Іншими словами, потрібно створювати

прив'язку міток до FEC для потоків, які забезпечені резервованими ресурсами за допомогою протоколу RSVP. Можна розглядати сукупність пакетів, для яких було виконано резервування по протоколу RSVP, як сукупність пакетів, що належать деякому новому класу FEC.

4.5.3 Протоколи маршрутизації, що використовуються в MPLS

Функції технології MPLS діляться на два компоненти: площина управління і площина пересилки пакетів. Компонент, що управляє, використовує протоколи маршрутизації для обміну маршрутною інформацією між маршрутизаторами. На основі цієї інформації в кожному маршрутизаторі формується і модифікується спочатку таблиця маршрутизації, а потім, з врахуванням інформації про суміжні системи в кожному інтерфейсі, – таблиця пересилки пакетів.

Тому першим кроком в алгоритмі функціонування мережі MPLS є формування таблиці маршрутизації, а потім заповнення в маршрутизаторах LSR таблиць міток, використовуваних при маршрутизації пакетів по мережі MPLS. Для цього в кожному з вузлів мережі з використанням протоколу маршрутизації створюється база топологічної інформації про мережні маршрути.

З цією метою можуть застосовуватися наступні протоколи маршрутизації:

- OSPF;
- IS-IS;
- BGP4.

4.5.3.1 Протокол OSPF

Протокол OSPF (Open Shortest Path First) - "першим вибирається найкоротший шлях" - відноситься до протоколів внутрішнього шлюзу IGP (Interior Gateway Protocol). До цієї категорії належать протоколи маршрутизації, що забезпечують обмін інформацією в межах автономної системи AS (Autonomous System є мережею, що знаходиться під єдиним адміністративним управлінням).

Розглянемо поняття метрики OSPF.

У OSPF використовується принцип контролю стану каналу (link-state protocol) за допомогою метрики. Метрика є оцінкою ефективності зв'язку в цьому каналі: чим менше метрика, тим ефективніше організація зв'язку. У простому випадку метрика маршруту може дорівнювати його довжині в пересилках (hops), як це відбувається в протоколі RIP. Але в загальному випадку значення метрики можуть визначатися в набагато ширшому діапазоні.

Метрика, що оцінює пропускну спроможність каналу, визначається, наприклад, компанією CISCO, як кількість секунд, що потрібно для передачі 100 Мбіт. Є наступна формула для обчислення метрики доставки інформації через канали мережі OSPF:

метрика $=10^8$/щвидкість передачі в бітах в секунду.

За цією формулою обчислені, наприклад, наступні метрики:

- канал із швидкістю 100 Мбіт/с відповідає метриці 1;
- мережа Ethernet / 802.3 відповідає метриці 10;
- тракт E1 2,048 Мбіт/с відповідає метриці 48;
- тракт T1 1,544 Мбіт/с відповідає метриці 65;
- канал 64 Кбіт/с відповідає метриці 1562;
- канал 56 Кбіт/с відповідає метриці 1785;
- канал 19,2 Кбіт/с відповідає метриці 5208;
- канал 9,6 Кбіт/с відповідає метриці 10416.

Крім того, протокол OSPF дозволяє визначити для будь-якої мережі значення метрики залежно від типа послуги ToS (Type of Service). Для кожної з метрик протокол OSPF будує окрему таблицю маршрутизації. Частіше всього OSPF вибирає маршрут на підставі смуги пропускання каналу.

Завантаження каналу є величиною, яка змінюється залежно від використання каналу, причому інтенсивна експлуатація каналу підвищує його завантаження, і тому при маршрутизації буває доцільно вибирати менш навантажені канали. Ще одна можлива метрика – затримка – визначає час в мікросекундах, який потрібний маршрутизатору для обробки, установки в чергу і передачі пакетів.

У разі, коли є декілька маршрутів з однаковим значенням метрики, маршрутизатори можуть використовувати для передачі пакетів всі ці маршрути, забезпечуючи балансування навантаження. Маршрутизатор OSPF поміщає в таблицю маршрутизації всі маршрути з однаковими значеннями метрики, і балансування навантаження між маршрутами відбувається автоматично. Стандартизований порядок розрахунку метрик, що оцінюють надійність, затримку і вартість, поки не визначений. Ці питання вирішуються адміністратором мережі.

Отже, OSPF є протоколом, заснованим на контролі стану каналів, поширюючим цю інформацію і що визначає на її основі маршрути найменшої вартості в заданій метриці. Саме з його допомогою LSR відображує видимий йому граф домена мережі MPLS, де для кожної пари суміжних вершин графа (маршрутизаторів) вказано ребро (канал), що їх сполучає, і метрику цього ребра. Граф вважається орієнтованим, якщо ребро, сполучаюче LSR1 з LSR2, і ребро, сполучаюче LSR2 з LSR1, можуть бути різними, або це може бути одне і те ж ребро, але з різними метриками.

Маршрутизатор, що працює за протоколом OSPF, виконує послідовно три операції: визначає стосунки сусідства і суміжності з іншими маршрутизаторами, обмінюється з ними OSPF-пакетами сповіщень про стан каналів LSA (link-state advertisement), формуючи таким чином повну топологічну карту мережі, а потім обчислює дерево маршрутів, використовуючи алгоритм "першим вибирається найкоротший шлях" SPF (Shortest Path First), відомий також як алгоритм Дейкстри.

Для мережі MPLS за допомогою цього алгоритму протокол OSPF, ґрунтуючись на базі даних про умови використання можливих зв'язків, обчислює найкоротші шляхи між заданою LSR – вершиною графа і всіма

останніми вершинами. Результатом роботи алгоритму є таблиця, де для кожної вершини графа мережі MPLS вказаний список ребер, що сполучають її зі всіма іншими вершинами цього графа по найкоротшому шляху.

Суть алгоритму ілюструє наступна процедура. Представимо змальовану на рис. 4.16 мережу MPLS, що містить 7 LSR, як набір з 7 фішок, лежачих на поверхні столу і сполучених між собою нитками різної довжини. Хай, наприклад, алгоритм Дейкстри виконується в маршрутизаторі LSR4. Поступово піднімаємо із столу фішку, відповідну LSR4. Нитки, що пов'язують цю фішку з іншими, починають натягатися, і наступною із столу буде піднята фішка LSR2, пов'язана з LSR4 найкоротшою ниткою. При подальшому підйомі фішки LSR4 ми піднімемо з поверхні столу і фішку LSR5. Найкоротший (у розглянутому вище сенсі) шлях між LSR4 і LSR5 представить або нитка, що зв'язує відповідні цим двом LSR фішки безпосередньо, або складений шлях з ниток між фішками LSR4 і LSR2, LSR2 і LSR3, LSR3 і LSR5. Продовжуючи процедуру підйому фішки LSR4, ми крок за кроком піднімемо всі фішки, знаходячи кожного разу найкоротший шлях між LSR4 і тим LSR, якому відповідає чергова фішка, що піднімається ниткою.

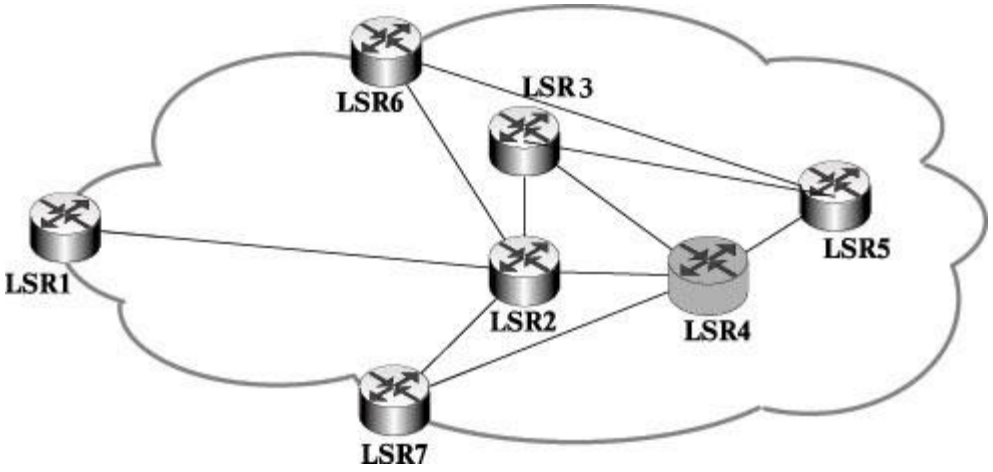


Рис. 4.16 - Ілюстрація алгоритму Дейкстри

Існує два різні маршрути між LSR4 і LSR5: прямий і складений з ділянок між LSR4 і LSR2, LSR2 і LSR3, LSR3 і LSR5. В тому випадку, якщо між двома вузлами мережі існує декілька маршрутів з близькими за значенням метриками, протокол OSPF дозволяє розподіляти трафік по цих маршрутах в пропорції, відповідній значенням метрик. Наприклад, якщо прямий маршрут між LSR4 і LSR5 має метрику 4, а складений маршрут з ділянок LSR4 і LSR2, LSR2 і LSR3, LSR3 і LSR5 має метрику 8, то дві третини трафіку буде направлено по першому з них, а третина, що залишилася, – по другому.

Сумарний ефект такого рішення полягає в зменшенні середньої затримки проходження дейтаграм від відправника до одержувача, а також в згладжуванні коливань затримки.

Ще одна перевага підтримки альтернативних маршрутів пов'язана з міркуваннями надійності. Коли використовується лише один з можливих маршрутів і він раптово виходить з ладу, весь трафік має бути терміново

перекладений на альтернативний маршрут. При масовому перемиканні великих об'ємів трафіку з одного маршруту на іншій можливі великі втрати і навіть утворення затору на новому маршруті. Якщо ж до аварії використовувалося розподіл трафіку по декількох маршрутах, відмова одного з них викличе ремаршрутизацію лише частини трафіку, і це може згладити негативні наслідки аварії.

Логічна підсистема автономної системи, в якій OSPF функціонує як протокол внутрішньої маршрутизації, називається *областю OSPF* (OSPF area). Області "укрупнюють" маршрутну інформацію протоколу OSPF і допомагають приховувати деталі топології мережі. Так, топологія однієї області не відома ні в якій іншій області. Внутрішні маршрутизатори області взагалі не володіють інформацією про топологію використовуючих мереж OSPF, які знаходяться за межами цієї області, що дає виграш у витратах на підтримку маршрутної інформації. Це робить OSPF добре масштабованим протоколом маршрутизації для крупних мереж. А сам протокол OSPF засновано на концепції областей як сукупностей суміжних мереж і маршрутизаторів, що відносяться до них, з інтерфейсами, що пов'язують їх з цими мережами і з вузлами в них.

Автономна система, що базується на протоколі OSPF, може бути однією областю або складатися з декількох областей. У кожній області працює власна копія алгоритму маршрутизації за станом каналів, що дозволяє кожній області формувати свою базу даних мережної топології. Саме область обмежує межі лавинної розсилки повідомлень, оскільки повідомлення не виходять за границі області, в якій вони були сформовані.

> *Примітка. Протокол OSPF розмежовує функції маршрутизаторів залежно від того, яке місце вони займають в автономній системі OSPF, об'єднуючій всі маршрутизатори, які ведуть обмін інформацією під управлінням загального протоколу. Зрозуміло, маршрутизатори розділяються на класи протоколу OSPF, а не технології MPLS, але оскільки всі маршрутизатори MPLS підтримують протокол OSPF (якщо він вибраний як протокол, за допомогою якого складається топологічна карта мережі), подібна класифікація повністю до них застосовна. Таким чином, терміни "маршрутизатор LSR" і " OSPF - маршрутизатор" використовуються як синоніми.*

З точки зору протоколу OSPF, є маршрутизатори чотирьох типів:

- внутрішній маршрутизатор IR (Internal Router), всі інтерфейси якого знаходяться усередині однієї області OSPF ;
- маршрутизатор опорної області BR (Backbone Router), всі інтерфейси якого знаходяться усередині опорної області;
- пограничний маршрутизатор області ABR (Area Border Router), розташований на границі двох областей OSPF ;
- граничний маршрутизатор автономної системи ASBR (Autonomous System Boundary Router), який розташовується на межі двох автономних систем, що підтримують OSPF.

Окрім цього призначаються два маршрутизатори, так і звані: призначений маршрутизатор DR (Designated Router) і резервний призначений маршрутизатор BDR (Backup Designated Router), які є центральними вузлами збору всіх

повідомлень про коректування. Всі останні маршрутизатори є по відношенню до маршрутизаторів DR і BDR підлеглими. Причому, один і той же маршрутизатор може виконувати в системі декілька функцій одночасно.

Розглянемо стисло принцип функціонування OSPF.

Перший етап - ініціювання. Спочатку розповсюджується інформація про топологію мережі, ініціюються відношення сусідства і суміжності і будується граф мережі. Після ініціації кожен OSPF-маршрутизатор починає обмін повідомленнями про стан каналів LSA, передає пакети HELLO через всі свої інтерфейси, поширюючи цю інформацію по всіх сусідніх маршрутизаторах, так що кожен з них взнає ідентифікатори своїх найближчих сусідів. Ця топологічна інформація починає поширюватися по мережі від сусіда до сусіда, поповнюючи топологічні карти в маршрутизаторах LSR новими даними, і через деякий час досягає самих віддалених маршрутизаторів. В результаті всі маршрутизатори мережі отримують відомості про граф мережі, які зберігаються в їх топологічних базах даних.

Згодом, при появі нового зв'язку або нового сусіда, маршрутизатор дізнається про це з нових пакетів HELLO. У них вказується досить детальна інформація про той маршрутизатор, який передав цей пакет, а також про його найближчих сусідів, так що цей маршрутизатор можна однозначно ідентифікувати.

Таким чином, на першому кроці кожен маршрутизатор OSPF будує граф зв'язків мережі, в якому вершинами графа є маршрутизатори, а ребрами – канали, включені в інтерфейси маршрутизаторів. Для побудови цього графа всі маршрутизатори обмінюються зі своїми сусідами тією інформацією про мережу, яку вони мають в своєму розпорядженні на даний момент.

Другий етап - за допомогою отриманого графа знаходяться оптимальні маршрути, причому кожен маршрутизатор вважає себе центром мережі і шукає оптимальний маршрут до кожного відомого йому маршрутизатора (або до відомої йому мережі). У будь-якому знайденому таким чином маршруті, відповідно до принципу однокрокової маршрутизації, запам'ятовується лише перший крок – до наступного маршрутизатора. Якщо декілька маршрутів до мережі призначення мають однакову метрику, то в таблиці маршрутизації запам'ятовуються перші кроки всіх цих маршрутів. Дані про ці кроки потрапляють в таблицю маршрутизації. Завдяки ієрархічній структурі областей зменшуються перевантаження, пов'язані з підтримкою величезних таблиць маршрутизації і з перерахунком цих таблиць при змінах маршрутів. Сповіщення про коректування передаються лише в разі, якщо в мережі відбуваються зміни. Ці сповіщення розсилаються всім маршрутизаторам OSPF, що скорочує час збіжності.

4.5.3.2 Протокол IS-IS

Протокол маршрутизації IS-IS (Intermediate System - to - Intermediate System) - протокол обміну даними між проміжними системами - використовує той же принцип маршрутизації за станом каналів, що і

розглянутий вище протокол OSPF. Але якщо OSPF є розробкою IETF, то протокол IS-IS був створений ISO (International Standard Organization).

В термінології ISO маршрутизатори називаються "Проміжними системами" (Intermediate System, IS), а хости – "кінцевими системами" (End System, ES). Існує також протокол ES-IS, за допомогою якого маршрутизатори дізнаються про підключені до них хости, а хости – про маршрутизатори. У технології MPLS протокол IS-IS застосовується майже так само, як і розглянутий вище протокол OSPF. Обидва вони відносяться до класу протоколів IGP і служать для створення і підтримки топологічної карти, використовуваної протоколом LDP. Практика показала, що протокол IS-IS дуже добре працює у вельми великих мережах, що містять більше 500 маршрутизаторів [4].

Подібно OSPF, протокол IS-IS розділяє мережу на області, аби не поширювати інформацію про маршрути серед всіх маршрутизаторів мережі, забезпечуючи розумні розміри їх таблиць маршрутизації, а тим самим - швидку збіжність пошуку маршруту. Протоколи динамічної маршрутизації задіяні в LSR з метою ідентифікувати сусідні LSR одного мережного домена і періодично оновлювати інформацію про топологію мережі за допомогою розглянутих сповіщень про стан каналів. Це є і головною перевагою такої маршрутизації, оскільки для передачі даних між двома кінцевими пунктами використовується найкоротший на даний момент маршрут.

Означена перевага протоколу IS-IS – в той же час і його істотний недолік. Цей недолік пов'язаний з так званою лавинною розсилкою пакетів (flooding), що викликається раптовою зміною стану каналів (або канал несподівано став недоступний, або, навпаки, відновив свою роботу після перерви). Flooding характеризується обміном між маршрутизаторами величезною кількістю службових пакетів, оскільки кожен маршрутизатор, сусідній з даним, прийнявши чергове сповіщення про зміну стану каналів і відновивши свої таблиці маршрутизації, пересилає його далі. У IS-IS присутні аналогічні OSPF механізми виявлення сусідів за допомогою пакетів HELLO, синхронізації баз даних і сповіщення про зміну стану зв'язку шляхом розсилки пакетів (flooding).

Основна метрика, використовувана в IS-IS, – це деяке число, що не перевищує 1024 для маршруту і 64, – для каналу. Числові значення цієї метрики для кожного каналу і маршруту визначає системний адміністратор. Метрика маршруту обчислюється як сума метрик складових його каналів. Крім того, можна задати три додаткові метрики: "затримка" (delay), що відображає тривалість затримки в каналі, "вартість передачі по каналу" (expense), що відображає комунікаційні витрати, і "помилки" (error), відображає коефіцієнт помилок в каналі.

Принципи маршрутизації IS-IS дуже схожі на використовувані в протоколі OSPF. Протокол IS-IS підтримує і дворівневу ієрархічну систему мереж

(периферійні області і магістральна область), але принцип організації цієї системи відрізняється від принципу її організації в OSPF.

4.5.3.3 Протокол BGP

Протокол BGP (Border Gateway Protocol) – протокол граничного шлюзу. Розглянемо лише основні функції протоколу, які безпосередньо використовуються в технології MPLS. Зокрема, це відноситься до багатопротокольного розширення протоколу BGP -4, що знайшов впровадження при побудові MPLS -VPN.

У технології MPLS використовуються протоколи маршрутизації OSPF, IS-IS і BGP-4 для обміну інформацією про маршрути між маршрутизаторами. На основі цієї інформації в кожному маршрутизаторі формується і модифікується спочатку таблиця маршрутизації, а потім, з врахуванням інформації про суміжні системи в кожному інтерфейсі, – таблиця пересилки пакетів.

Але якщо врахувати, що розглянуті вище протоколи OSPF і IS-IS виконують це завдання в межах однієї автономної системи AS, яка є, по суті, самодостатньою незалежною мережею, не маючої отриманих яким-небудь логічним шляхом відомостей про інші мережі у складі всієї мережі MPLS, то роль протоколу BGP -4 є набагато ширшою. Його основне призначення якраз і полягає в тому, аби передавати від одного BGP-маршрутизатора іншим BGP-маршрутизаторам інформацію про наявність інших автономних мереж і про їх структуру, формуючи тим самим ієрархічну схему маршрутизації, що зв'язує різні вузли і автономні мережі в єдину MPLS-мережу і дозволяє вільно встановлювати зв'язок між собою системам, невідомим одна одної.

Необхідність декомпозиції глобальної IP/MPLS-сети на автономні системи обумовлена тим, що трафік може перевищити всі допустимі межі, якщо велика кількість маршрутизаторів спробує вступити у взаємодію одночасно.

BGP специфікується як сеанс зв'язку між двома вузлами. В ході BGP - сеансу між одноранговими вузлами протоколу BGP відбувається обмін повідомленнями за TCP - з'єднанням.

Версія 4 протоколи BGP включає два окремі протоколи:

- протокол EBGP (External Border Gateway Protocol), використовуваний для маршрутизації між автономними системами;
- протокол IBGP (Internal Border Gateway Protocol), використовуваний для маршрутизації усередині автономної системи.

Принципова відмінність протоколу BGP від OSPF і IS-IS полягає в тому, що він відноситься не до категорії протоколів маршрутизації за станом каналів, а до категорії дистанційно-векторних протоколів.

Принцип вектора відстані має на увазі вибір маршруту виходячи з найкоротшого відстані між системами, визначуваної числом пересилок. Протоколи на основі вектора відстані зазвичай враховують лише число пересилок (hops) в маршруті. Окрім звичайних параметрів дистанційно-векторних протоколів в BGP використовується додатковий механізм, що іменується маршрутно-векторною маршрутизацією (path-vector routing). Це обумовлено тим, що ні маршрутизація з врахуванням стану каналів, ні

дистанційно-векторна маршрутизація в чистому вигляді для зовнішньої маршрутизації не ефективні.

Метод дистанційно-векторної маршрутизації інколи називають також методом Беллмана або методом Форда-Фалкерсона по імені дослідників, які першими опублікували ідею алгоритму. Сама ця ідея досить проста. Маршрутизатор зберігає в таблиці список всіх відомих маршрутів з вказівкою в кожному елементі таблиці мережі одержувача і цілого числа – кількості пересилок до цієї мережі. Час від часу кожен маршрутизатор посилає копію своєї таблиці іншим маршрутизаторам, до яких він має прямий доступ. Отримавши таку копію від LSR-B, маршрутизатор LSR-A аналізує отриманий набір адресатів і відстаней до них. Маршрутизатор LSR-A замінює дані в своїй таблиці, якщо маршрутизатору LSR-B відомий коротший, ніж наявний в ній, маршрут до одержувача, або якщо в його списку невідомий йому до цих пір одержувач, а також якщо LSR-A виконує маршрутизацію через LSR-B, але відстань від LSR-B до одержувача змінилася.

На основі цієї таблиці, згідно алгоритму Беллмана-Форда, і розраховується значення метрики (наприклад вартості маршруту, затримки і тому подібне) для кожної пересилки в мережі і пошук мінімального сумарного числа пересилок. Звернемо увагу на те, що поняття "Дистанційний вектор" пов'язане з характером періодично передаваної протоколом інформації. У повідомленнях міститься пара чисел {R, D}, де R – вектор, що визначає одержувача, а D – відстань до цього одержувача, тобто один маршрутизатор повідомляє інший про свою можливість досягти одержувача R за D пересилок.

При маршрутизації за протоколом BGP пересилка можлива як між внутрішніми маршрутизаторами (розташованими усередині однієї AS), які працюють під управлінням протоколу IBGR так і між зовнішніми маршрутизаторами, що з'єднують різні автономні системи AS, коли маршрутизація виконується під управлінням протоколу EBGP.

Маршрутно-векторний механізм, що використовується в BGP, допомагає вирішити проблему традиційної дистанційно-векторної маршрутизації, що виникає в умовах функціонування між автономними системами. Річ у тому, що в різних AS можуть застосовуватися різні метрики виміру довжини маршрутів, а це може привести до проблем інтерпретації одних і тих же числових значень в зовнішніх BGP -маршрутизаторах. Тому механізм маршрутно-векторної маршрутизації передбачає відмову від метрики маршруту. Тоді маршрутизатори просто обмінюються інформацією про автономні системи, до яких і через яких у них є доступ.

Існує три класи автономних систем AS:

- системи з множинною адресацією (multihomed);
- тупикові, такі, що мають лише один вихід в Інтернет (single-homed);
- багатоканальні транзитні мережі (multihomed transit).

Системи з множинною адресацією (multihomed) – це системи, що мають декілька з'єднань із зовнішніми автономними системами. Такі системи ще називають багатоканальними нетранзитними (multihomed nontransit). Автономна

система з множинною адресацією може приймати маршрутну інформацію від всіх сполучених з нею систем, але сама вона виконує лише внутрішню маршрутизацію.

Багато автономних систем насправді є тупиковими (stub) або одноканальними (single-homed) і мають лише один вихід в зовнішню мережу. Відповідно, вони не вимагають жодних додаткових правил для управління ними і обслуговування великого списку BGP - маршрутів.

Третій тип автономної системи – транзитна мережа. Транзитні AS – це системи з множинною адресацією, які приймають інформацію від зовнішніх автономних систем і виконують маршрутизацію цієї інформації до інших зовнішнім AS.

Розглянемо основні типи маршрутизаторів BGP. Є три типи маршрутизаторів BGP:

- спікери;
- граничні шлюзи;
- рівноправні маршрутизатори BGP.

Спікерами BGP (BGP speakers) є всі маршрутизатори автономної системи BGP. Спікери BGP, що з'єднують дві або декілька автономних систем, називаються граничними шлюзами (Border Gateways). Вони потрібні автономним системам лише в тому випадку, якщо AS використовує для зв'язку з іншими автономними системами IP/MPLS-мережі протокол EBGR. Завдання граничного шлюзу – сповіщати про внутрішні маршрути автономної системи (і про інші відомі йому маршрути) будь-який зовнішній спікер BGP, з яким цей шлюз зв'язаний. Згідно принципам мережної маршрутизації, під час сеансів зв'язку спікери BGP обмінюються маршрутною інформацією про топологію і метричні характеристики відповідних ділянок мережі. Такий обмін відбувається між рівноправними маршрутизаторами (BGP-peer) автономної системи.

Рівноправні маршрутизатори BGP не обов'язково повинні мати прямі зв'язки один з одним; проте між двома спікерами BGP завжди повинен існувати стандартний спосіб комунікації для того, щоб вони могли ініціювати сеанс зв'язку.

Коли BGP встановлює сеанс зв'язку двох рівноправних маршрутизаторів, між якими немає прямого з'єднання, такий зв'язок називається одноранговим зв'язком з пересилкою за протоколом EBGP (EBGP multihop peering). Використовуючи зовнішні з'єднання за протоколом EBGP, спікер BGP може ініціювати сеанс зв'язку з іншими спікерами, що знаходяться на відстані декількох пересилок. У всіх таких випадках для організації сеансів BGP використовує протокол TCP. При одноранговому зв'язку спікери BGP обмінюються повними копіями таблиць маршрутизації під час первинного двостороннього сеансу, включаючи повторні запуски.

BGP є протоколом із стійким станом, це означає, що в разі успішного обміну маршрутною інформацією між одноранговими вузлами, не вимагається її оновлення, тобто ця інформація вважається дійсною до тих пір, поки один з однорангових вузлів не повідомить інший про те, що це не так, або доки не закінчиться BGP -сеанс між ними.

Ключовим принципом протоколу BGP, є те, що коли один одноранговий вузол інформує свого партнера про те, що IP-адрес доступний по повідомленому маршруту, партнер може бути упевнений, що рівноправний вузол вже успішно використовує цей маршрут для передачі власного трафіку. При цьому мається на увазі, що маршрути, про які вузол сповіщений, можуть використовуватися завжди, коли про них оголошується. Разом з можливістю використовувати маршрут надається набір атрибутів, пов'язаних з IP-префіксом.

Протокол EBGP (Exterior Border Gateway Protocol) використовується для встановлення з'єднання між спікерами BGP різних автономних систем, включаючи комунікації між Інтернет-провайдерами і точками доступу PoP (Point of presence), а також між великими корпоративними мережами і провайдерами послуг.

Вочевидь, що BGP -маршрутизаторы, що знаходяться в одній AS, теж повинні обмінюватися між собою маршрутною інформацією. Це необхідно для погодженого відбору зовнішніх маршрутів відповідно до політики даної AS і для організації транзитних маршрутів через автономну систему. Такий обмін проводиться по протоколу BGP, який в цьому випадку називається IBGP (Internal BGP).

Відмінність IBGP від EBGP полягає в тому, що при сповіщенні про маршрут сусіднього маршрутизатора, що знаходиться в тій же AS, в список номерів автономних систем не вводиться номер власної автономної системи.

4.6 Віртуальні приватні мережі (VPN) MPLS

4.6.1 Огляд основних технологій побудови VPN

Віртуальна мережа VPN (Virtual Private Network) – віртуальна приватна мереж а) – узагальнена назва технологій, що дозволяють створювати логічну мережу на базі загальнодоступної мережі (поверх іншої мережі, наприклад, Інтернет), що підтримує конфіденційність передаваної інформації за рахунок використання тунелювання, шифрування і інших процедур захисту. Внаслідок чого створюється закритий для сторонніх канал обміну інформацією. VPN дозволяє об'єднати, наприклад, декілька географічно віддалених мереж організації в єдину мережу з використанням для зв'язку між ними непідконтрольних каналів.

Всі мережі VPN умовно можна розділити на три основні види:

- внутрішньокорпоративні VPN (Intranet VPN);
- міжкорпоративні VPN (Extranet VPN):
- VPN з віддаленим доступом (Remote Access VPN).

Інтрамережа є найбільш простим варіантом VPN, він дозволяє об'єднати в єдину захищену мережу декілька розподілених філій однієї організації, що взаємодіють по відкритих каналах зв'язку.

Екстрамережа – варіант побудови VPN, призначений для забезпечення доступу з мережі однієї компанії до ресурсів мережі іншої, рівень довіри до якої набагато нижчий, ніж до своїх співробітників. Тому, коли декілька компаній приймають рішення працювати разом і відкривають один для одного свої мережі, вони повинні врахувати, що їх нові партнери повинні мати доступ лише до певної інформації.

VPN з віддаленим доступом. Принцип роботи VPN з віддаленим доступом простий: користувачі встановлюють з'єднання з місцевою точкою доступу до глобальної мережі (PoP), після чого їх виклики передаються за допомогою тунелю через Інтернет, що дозволяє уникнути плати за міжміський і міжнародний зв'язок. Потім всі виклики концентруються на відповідних вузлах і передаються в корпоративні мережі.

Важливу роль при побудові VPN грають стосунки підприємства з провайдером, зокрема, розподіл між ними функцій по конфігурації і експлуатації VPN -пристроїв. При створенні захищених каналів VPN-засоби можуть розташовуватися як в середовищі устаткування провайдера, так і в устаткуванні підприємства. Залежно від цього виділяють два варіанти побудови VPN:

- схема користувача (Customer Provided VPN);
- схема провайдера (Provider Provisioned VPN).

Окрім вищепереліченої класифікації, всі варіанти створення VPN можна розділити на дві категорії: програмні і апаратні.

Програмні рішення є готовими додатками, які встановлюються на підключеному до мережі комп'ютері із стандартним програмним забезпеченням.

Апаратні VPN-рішення включають комп'ютер, операційну систему, спеціальне програмне забезпечення.

Віртуальні приватні мережі можна вважати повноцінним видом транспорту для передачі трафіку, лише якщо є гарантії на пропускну спроможність і інші параметри продуктивності, а також на безпеку передаваних даних.

Розглянемо функції VPN щодо захисту даних.

Підключення будь-якої корпоративної мережі до публічної викликає погрози двох типів:

- несанкціонований доступ до ресурсів локальної мережі, отриманий в результаті входу в цю мережу;
- несанкціонований доступ до даних при передачі трафіку по публічній мережі.

Для створення захищеного каналу засобу VPN використовують процедури шифрування, аутентифікації і авторизації.

- Шифрування. Методів шифрування досить багато, тому поважно, аби на кінцях тунелю використовувався один і той же алгоритм шифрування. Крім того, для успішної дешифровки даних джерелу і одержувачеві даних необхідно обмінятися ключами шифрування. Слід зазначити, що шифрування повідомлень необхідне не завжди. Часто воно виявляється досить дорогою процедурою, що вимагає додаткових приставок для

маршрутизаторів, без яких вони не можуть одночасно з шифруванням забезпечувати прийнятний рівень швидкодії.

- Аутентифікація. Під аутентифікацією розуміється визначення користувача або кінцевого пристрою. Аутентифікація дозволяє встановлювати з'єднання лише між легальними користувачами і, відповідно, запобігає доступу до ресурсів мережі несанкціонованих користувачів. У процедурі беруть участь дві сторони: одна доводить свою автентичність, а інша її перевіряє і приймає рішення.
- Авторизація. Авторизація врахоаує надання абонентам різних видів послуг. Кожному користувачеві надаються визначені адміністратором права доступу. Ця процедура виконується після процедури аутентифікації і дозволяє контролювати доступ санкціонованих користувачів до ресурсів мережі.

До основних технологій побудови VPN можна назвати такі технології, як: IPSec VPN, MPLS VPN, VPN на основі технологій туннелювания PPTP і L2TP. У всіх перерахованих випадках трафік посилається в мережу провайдера за протоколом IP, що дозволяє провайдерові надавати не лише послуги VPN, але і різні додаткові сервіси (контроль за роботою клієнтської мережі, хостинг Web і поштових служб, хостинг спеціалізованих застосувань клієнтів).

Internet Protocol Security (IPSec) відноситься до найбільш поширених і популярних технологій VPN. Стандарт IPSec забезпечує високу міру гнучкості, дозволяючи вибирати потрібний режим захисту, а також дозволяє використовувати різні алгоритми аутентифікації і шифрування даних. Режим інкапсуляції пакетів дає можливість ізолювати адресні простори клієнта і провайдера за рахунок вживання двох IP адрес – зовнішнього і внутрішнього.

IPSec, як правило, застосовується для створення VPN, підтримуваних провайдером, – тунелі в них будуються на базі пристроїв клієнта, але конфігуруються вони віддалено і управляються провайдером. Технологія IPSec дозволяє вирішувати завдання по встановленню і підтримці захищеного каналу, а саме аутентифікацію користувачів або комп'ютерів при ініціалізації каналу, шифрування і аутентифікацію передаваних даних між кінцевими точками каналу.

Недоліком даної технології є той факт, що зі всіх властивостей віртуальної мережі технологія IPSec реалізує лише захищеність і ізольованість адресного простору. Пропускну спроможність і інші параметри QOS вона не підтримує. Крім того, мінусом IPSec є і його орієнтованість виключно на IP-протокол.

VPN на основі тунелювання через IP включає всі технології для утворення VPN, які використовують тунелі через IP-мережі. Використання тунеля дозволяє ізолювати адресний простір клієнта, що у свою чергу дає клієнтові можливість переносити незашифрований трафік (L2TP) або шифрувати його (PPTP). Протокол PPTP підтримує управління потоками даних і багатопротокольне тунелювання на базі протоколу IP. Віддаленим користувачам протокол дозволяє отримати доступ до корпоративної мережі, підключаючись по телефонній лінії до місцевого постачальника послуг Інтернет замість прямого підключення до

мережі компанії. PPTP забезпечує з'єднання з потрібним сервером, створюючи для кожного віддаленого клієнта віртуальну мережу. Протокол вирішує багато проблем мережних адміністраторів, вимушених забезпечувати підтримку безлічі віддалених користувачів, але бажаючих уникнути створення і обслуговування відносно дорогої мережі на виділених каналах.

Специфікації L2TP розробляє IETF. Він орієнтований на підтримку багатопротокольного тунелювання, але окрім цього забезпечує сумісність всіх L2TP-продуктов. До недоліків протоколів PPTP і L2TP можна віднести відсутність вбудованих алгоритмів шифрування.

4.6.2 Пакетні віртуальні приватні мережі MPLS

Технологія MPLS в даний час є одній з найбільш перспективних технологій створення VPN. Використання MPLS для побудови VPN дозволяє сервіс-провайдерам швидко і економічно створювати захищені віртуальні приватні мережі будь-якого розміру в єдиній інфраструктурі.
Функції VPN спільно з багатопротокольною комутацією по мітках (MPLS) дозволяють реалізувати в мережі провайдера розширювані магістральні VPN-служби 3-го рівня на базі протоколу IPv4.

Мережа MPLS VPN ділиться на дві області: IP-мережі клієнтів і внутрішня (магістральна) мережа провайдера, яка служить для об'єднання клієнтських мереж. У загальному випадку у кожного клієнта може бути декілька територіально відособлених мереж IP, кожна з яких у свою чергу може включати декілька підмереж, зв'язаних маршрутизаторами. Такі територіально ізольовані мережні елементи корпоративної мережі прийнято називати сайтами. Сайти, що належать одному клієнтові, обмінюються IP-пакетами через мережу провайдера MPLS і утворюють віртуальну приватну мережу цього клієнта. Обмін маршрутною інформацією в межах сайту здійснюється по одному з внутрішніх протоколів маршрутизації IGP.

Структура MPLS VPN передбачає наявність таких основних компонентів технології MPLS, використовуваних для створення VPN-мереж:

- Customer Edge Router, CE – граничний маршрутизатор клієнта (Edge LSR в термінології MPLS);
- Provider Router, P – внутрішній маршрутизатор магістральної мережі провайдера (LSR в термінології MPLS);
- Provider Edge Router, PE – граничний маршрутизатор мережі провайдера.

Базові маршрутизатори MPLS (P). Базові маршрутизатори або внутрішні маршрутизатори магістральної мережі провайдера (LSR в термінології MPLS), не містять маршрутів VPN-мереж. Разом з іншими LSR-пристроями провайдера вони зазвичай утворюють повнозв'язну або частково-зв'язну топологію і здійснюють інтерфейс з граничними маршрутизаторами провайдера (provider edge - PE

router). Р-маршрутизатори ніколи не приєднуються безпосередньо до маршрутизаторів користувача.

Граничні маршрутизатори мережі MPLS (PE). Маршрутизатори точок присутності, також відомі як граничні маршрутизатори провайдера (Provider Edge router - PE router), містять VPN-маршрути для підтримуваних ними мереж VPN. Вони підтримують інтерфейс з базовими маршрутизаторами провайдера. До PE-маршрутизатору може бути підключені декілька CE-маршрутизаторів, що знаходяться в різних сайтах і навіть відносяться до різних VPN.

Граничні маршрутизатори користувача (Customer Edge router – CE router). Граничним маршрутизаторам користувача не потрібні функції MPLS, а для підтримки з'єднань вони можуть використовувати звичайні методи маршрутизації. Рангова модель вимагає, аби вузол користувача підтримував паритетний зв'язок лише з PE-маршрутизатором CE-маршрутизатори ніколи безпосередньо не під'єднуються до Р-маршрутизаторам. CE-маршрутизатор відноситься до одного сайту, але сайт може належати до декількох VPN.

Маршрутизатори користувача (Customer router – C-router). Внутрішнім маршрутизаторам, що належать користувачеві, також званим С-маршрутизаторам і, не потрібно підтримувати функції MPLS, а для підтримки з'єднань між собою і з CE-маршрутизаторами вони можуть використовувати звичайні методи маршрутизації.

VPN-мережі включають пристрої користувача, приєднані до CE-маршрутизаторів. CE-маршрутизатори, що належать до будь-якої з VPN-мереж, можуть бути приєднані до будь-якого з PE-маршрутизаторів провайдера. PE-маршрутизатори сполучені між собою через базову мережу Р-маршрутизаторів.

Маршрутизатори CE не зобов'язані підтримувати технологію багато-протокольної комутації, підтримка MPLS потрібна лише для внутрішніх інтерфейсів PE маршрутизаторів і, звичайно, для всіх інтерфейсів маршрутизаторів Р. За функціональною побудовою складнішими є граничні маршрутизатори мережі провайдера. На них покладається функція підтримки VPN, а саме, розмежування маршрутів і даних, що поступають від різних клієнтів. Крім того, ці маршрутизатори служать кінцевими точками шляхів LSP між сайтами замовника.

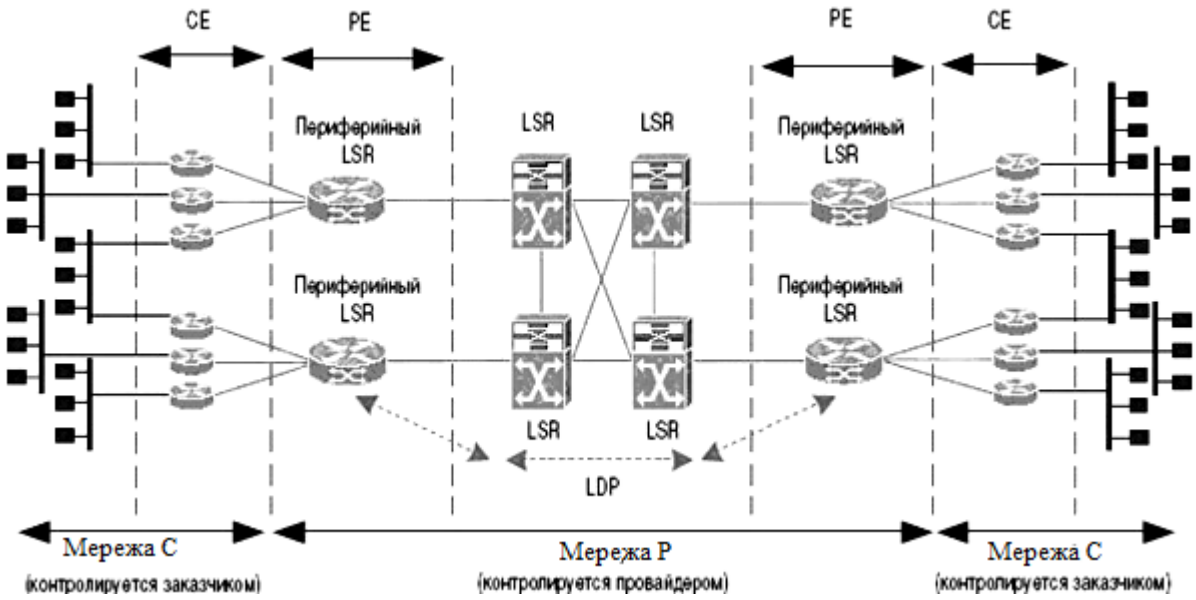


Рис. 4.17– MPLS VPN

Через маршрутизатори PE проходить невидима між зоною клієнтських сайтів і зоною ядра провайдера. По одну сторону розташовуються інтерфейси, через які PE взаємодіє з маршрутизаторами P, а по іншу – інтерфейси, до яких підключаються сайти клієнтів. З одного боку на PE поступають оголошення про маршрути магістральної мережі, з іншого боку – оголошення про маршрути в мережах клієнтів.

Кожен пристрій MPLS PE підтримує по одній таблиці VRF (VPN Routing and Forwarding instance –таблиця маршрутизації і передачі VPN) на кожну VPN. У таблиці VRF зберігаються дані про всі маршрути, відомі цьому пристрою в тій або інший VPN. Причому маршрутна інформація, що стосується конкретної VPN, міститься лише в PE маршрутизаторах, до яких приєднані сайти даної VPN. Таким чином вирішується проблема масштабування, що неминуче виникає в разі наявності цієї інформації у всіх маршрутизаторах мережі оператора. MPLS-пристрій ідентифікує маршрути, що відносяться до певної мережі VPN за допомогою "розрізнювача маршрутів" (Route Distinguisher - RD), який привласнюється всім маршрутам відповідного CE. Розрізнювач маршрутів (Route Distinguisher, RD) є префіксом, який додається всім адресам адресного простору однієї VPN і унікально ідентифікує цю VPN. В результаті на маршрутизаторі PE всі адреса, що відносяться до різних VPN, обов'язково відрізнятимуться один від одного, навіть якщо вони мають співпадаючу частину – адрес IP. Ці "розрізнювачі" (RD) мають значення лише для PE-пристроїв, оскільки P-маршрутизатори комутують чпрунки або пакети на підставі інформації, існуючої в мітках.

Кожен граничний маршрутизатор замовника повинен передати інформацію про свої маршрути у відповідні таблиці VRF, визначені в MPLS-мережі для даної VPN. Це завдання виконується граничними маршрутизаторами замовника, налаштованими на передачу інформації про маршрути, необхідні іншим сайтам своєї ж VPN. Для цієї передачі може використовуватися статична маршрутизація, а також маршрутизація BGP, OSPF або RIPv2.

Обмін маршрутною інформацією між сайтами кожною окремою VPN виконується під управлінням протоколу MP-BGP (Multiprotocol BGP).

Протокол MP-BGP використовується для обміну маршрутами безпосередньо між PE-маршрутизаторами і може переносити в маршрутній інформації адреси VPN-IPv4.

Специфікація RFC 2283 ("Багатопротокольні розширення для протоколу BGP4" — "Multiprotocol Extensions for BGP4"), дозволяє протоколу BGP передавати розширені атрибути. Ця технологія створює основу сучасних реалізацій середовищ MPLS, в яких PE-маршрутизатори зв'язуються один з одним за допомогою протоколу IBGP в базовій магістралі P-маршрутизаторів провайдера, які не беруть участь в роботі протоколу BGP. PE-маршрутизатори створюють повнозв'язну топологію протоколу IBGP.

Протокол BGP поширює серед PE-маршрутизаторів інформацію про досяжність для VPN-префіксів середовища IP версії 4 за допомогою розширень багатопротокольного BGP, які включають підтримку сімейств адрес, відмінних від адрес протоколу IP версії 4. Це здійснюється так, щоб маршрути VPN-мережі були відомі лише її членам, що дозволяє їм встановлювати зв'язок один з одним. Сімейство адрес створюється для того, щоб мульти-протокольний протокол граничного шлюзу (Multiprotocol Border Gateway Protocol — MP-BGP) міг передавати інформацію протоколів, відмінних від IP четвертої версії.

PE-маршрутизатори зв'язують адреса IPv4 конкретної C-мережі з новим сімейством адрес VPN-IPv4. Адрес VPN-IPv4 складається з 12 байтів. Перші 8 байтів називаються "Розрізнювачами маршруту" (Route Distinguisher - RD). Останні 4 байти містять оригінальний адрес IPv4. Якщо до однієї P-мережі підключено дві C-мережі і, якщо той або інший IP-адрес використовується в обох C-мережах, PE-маршрутизатори, підключені до цих C-мереж, перетворять однакові адреса IPv4 в два різних адреси VPNIPv4 (за допомогою використання різних RD). Таким чином, навіть якщо в двох C-мережах використовуються одні і ті ж адреса IPv4, відповідні ним адреса VPN-IPv4 відрізнятимуться один від одного. У P-мережі маршрути, що ведуть до адрес, що знаходяться в C-мережах, визначаються по адресах VPN-IPv4. Таким чином, збіги адрес в двох C-мережах не ведуть до невизначеності адресації в P-мережі. З іншого боку, якщо кінцева система має адрес, який є унікальним в межах мережі VPN, до якої ця система належить, їй абсолютно не потрібно знати про свій VPN-IPv4 адрес.

Дані про маршрути VPN-IPv4 для конкретної C-мережі передаються (за допомогою BGP) лише PE-маршрутизаторам, підключеним до цієї C- мережі. PE-маршрутизатори, які не підключені до C-сети, не отримують даних про її маршрути. В результаті об'єм інформації про маршрути, який зберігається на PE-маршрутизаторі, не пропорційний загальній кількості мереж VPN, підтримуваних в даній P-мережі. Цей об'єм пропорційний лише кількості мереж VPN, до яких безпосередньо підключений даний PE-маршрутизатор.

У MPLS-VPN вхідний PE-маршрутизатор повинен підтримувати окрему таблицю (forwarding table) для кожної С- мережі, до якої він підключений. Ця таблиця заповнюється даними про маршрути, що відносяться лише до цієї конкретної С- мережі. Дані про маршрути збираються через IBGP з інших вузлів PE, підключених до тієї ж С- мережі. Вхідний PE-маршрутизатор отримує IP-пакети від свого CE маршрутизатора. Далі він шукає "найкращий збіг" в VPN FIB, знаходить IBGP для наступного пристрою (PE2) і привласнює пакету стік міток (зовнішня мітка + внутрішня мітка). Все подальші P-маршрутизаторы комутують цей пакет лише на підставі зовнішньої мітки. Кінцевий PE-маршрутизатор видаляє зовнішню мітку і за допомогою внутрішньої мітки визначає, в яку мережу VPN/CE передати пакет. Після цього зовнішня мітка теж віддаляється, і пакет передається на підключений CE-маршрутизатор.

Маршрут, за яким пакет передається від вхідного до кінцевого PE-маршрутизатора, зазвичай включає один або декілька проміжних P-маршрутизаторів. Проміжні P-маршрутизатори не зберігають дані про маршрути VPN і не можуть доставити пакет до кінцевого IP-адресу. Правильне проходження пакету по P-мережі досягається за допомогою комутації по мітках. Якщо для пакету визначений крайовий PE-маршрутизатор, комутація по мітках направляє пакет саме до цього маршрутизатора. Вхідний PE-маршрутизатор привласнює пакету заголовок для комутації по мітках (зовнішню мітку), яка вказує маршрут (по P- мережі) до кінцевого PE-маршрутизатора. Проміжні P-маршрутизатори направляють пакет по цій мітці, а не за IP-адресом. Тому проміжні P-маршрутизатори і не повинні нічого знати про маршрутизацію в С-мережі. Вони також нічого не повинні знати про адреса VPN-IPv4. В принципі, P-маршрутизатори можуть одночасно підтримувати мережі MPLS-VPN і кінцеві пристрої LSR, що не мають до цих мереж жодного відношення.

Зовнішня мітка, яка використовується для маршрутизації пакету по P-мережі, вказує на маршрут до кінцевого PE-маршрутизатору. Внутрішня мітка, якою користується кінцевий PE-маршрутизатор, визначає кінцевий вихідний порт (або інтерфейс), через який необхідно передати пакет. Тому кінцевому PE-маршрутизатору також не потрібно знати IP-адрес, за яким передається пакет.

4.6.2.1 Таблиця VRF (VPN Routing and Forwarding instance – таблица маршрутизації і пересилки VPN).

Кожен PE-маршрутизатор підтримує одну або декілька таблиць маршрутів і пересилки VRF). Така таблиця підтримується для кожного сайту, підключеного до PE-маршрутизатору. Якщо IP-адрес пакету вказує на те, що його потрібно передати в сайт А, його шукають в таблиці (forwarding table) сайту А лише у тому випадку, коли пакет прибуває з сайту, що асоціюється з таблицею сайту А. Якщо сайт пов'язаний з декількома мережами VPN, його таблиця VRF може включати дані про маршрути всіх цих мереж. Наприклад, сайт CE1 належить до мереж VPNA і VPNB. В цьому випадку таблиця VRF пристрою PE1 міститиме інформацію про маршрути мережі VPNA і VPNB. Іншими словами, на пристрої PE1 не буде двох окремих таблиць VRF. Зазвичай на пристрої PE підтримується по одній таблиці VRF на сайт, навіть якщо з цим сайтом в даного пристрою є декілька з'єднань. Крім того, якщо різні сайти користуються одним і

тим же набором маршрутів, вони також об'єднуватимуться в одну таблицю VRF. Таблиці VRF на пристроях PE використовуються лише для пакетів, що поступають з сайту, безпосередньо підключеного до даного пристрою PE. Вони не використовуються для маршрутизації пакетів, що поступають з інших маршрутизаторів, встановлених в магістралі сервіс-провайдера. В результаті до одного і того ж адресу в мережі можуть вести декілька маршрутів, тому що маршрут для передачі кожного пакету визначається в точці, через яку пакет потрапляє в магістраль. Так, наприклад, один маршрут може використовуватися для передачі пакетів з мережі Екстранет (де встановлений міжмережний екран), а інший маршрут – для передачі пакетів за тим же адресом з мережі Інтранет.

4.6.2.2 Взаємодія між граничними маршрутизаторами PE і базовими маршрутизаторами P

Розглянемо взаємодію між граничними маршрутизаторами PE і базовими маршрутизаторами P. P-маршрутизатори підключаються до інших P-маршрутизаторів і до PE-маршрутизаторів. P-маршрутизатори виконують функції комутації по мітках. При цьому пакети передаються лише по мітках MPLS. У мережах MPLS-VPN для P-маршрутизаторів використовується дворівневий стек міток, за допомогою якого пакети передаються по магістралі з одного сайту VPN в інший. Зазвичай P-маршрутизатори зв'язуються один з одним за допомогою протоколу маршрутизації IGP (наприклад, IS-IS або OSPF) і не мають жодної інформації про інші маршрути, окрім маршрутів, які ведуть до PE-маршрутизаторів. PE-маршрутизатори вводять префікси своїх IP-адрес в магістральні таблиці маршрутизації IGP. Це дозволяє MPLS на кожному вузлі магістральної мережі привласнювати мітки, вказуючи на маршрут, що веде до того або іншого PE-маршрутизатору. Коли пристрій PE отримує пакет від пристрою CE, він вибирає певну таблицю VRF для пошуку адреса призначення для цього пакету. Якщо такий адрес знайдено і, якщо пакет призначений для пристрою CE, підключеного до даного PE-маршрутизатору, пакет прямує прямо на пристрій CE і не передається в магістраль. Якщо ж пакет не призначений для пристрою CE, підключеного до даного пристрою PE, для нього знаходиться наступний вузол (BGP Next Hop), а також мітка, яку цей вузол BGP наступної пересилки (Next-Hop) привласнив адресу призначення. Ця мітка записується в стек міток даного пакету і стає його внутрішньою міткою.

Якщо наступний вузол IGP (IBGP або OSPF) відрізняється від наступного вузла BGP, в стек записується додаткова мітка. Ця мітка вказує на наступний вузол BGP і стає зовнішньою міткою. (Якщо наступний вузол BGP збігається з наступним вузлом IGP, друга мітка може не привласнюватися).

Після цього MPLS доставляє пакет по магістралі до відповідного пристрою CE відповідно до зовнішньої мітки MPLS. Це означає, що всі рішення P-маршрутизаторів і PE-маршрутизаторів приймаються на основі даних MPLS, а IP-заголовок пакету не розглядається, доки пакет не поступить на кінцевий PE-маршрутизатор. P-маршрутизатор (або PE-

маршрутизатор), що знаходиться перед кінцевим PE-маршрутизатором, видаляє зовнішню мітку із стека MPLS і направляє пакет кінцевому PE-маршрутизатору. Кінцевий PE-маршрутизатор переглядає внутрішню мітку і відправляє пакет відповідному пристрою CE. Таким чином, до пристрою CE доходить звичайний IP-пакет, який не несе на собі жодних слідів MPLS.

MPLS не забезпечує безпеку за рахунок шифрування і аутентифікації, як це робить IPSec, але допускає вживання даних технологій як додаткових заходів захисту. Провайдер MPLS може пропонувати клієнтам послуги гарантованої якості обслуговування при використанні методів управління трафіком (Traffic Engineering) або диференційного обслговування (DiffServ).

Віртуальні мережі VPN MPLS орієнтовані на побудову захищеної корпоративної мережі клієнта на базі приватної мережної інфраструктури однієї компанії. Даний варіант організації поєднує в собі переваги вживання протоколу IP з безпекою приватних мереж і якістю обслуговування, що забезпечується технологією MPLS. Мережі MPLS VPN більш всього підходять для створення корпоративного простору для електронної комерції, що забезпечує єдине мережне середовище для підрозділів корпорації. Вони також можуть стати основою для електронної комерційної діяльності підприємства.

4.7 Управління трафіком в мережі MPLS (Traffic Engineering)

При будь-якому числі користувачів мережі NGN потрібне вирішення завдань по управлінню трафіком. В цієї мережі передбачається одночасне існування множини різнотипних потоків. Кожен з таких потоків вимагає безумовного дотримання одних параметрів передачі і допускає деякі поступки щодо інших. Тому в періоди виникнення перевантажень мережа може для одного потоку урізувати смугу пропускання, для іншого – збільшити час доставки, а для третього, наприклад, нехтувати цілісністю передаваних даних. Мультисервісна мережа повинна володіти складнішою системою управління в порівнянні з системами управління традиційними мережами. Вона повинна забезпечувати одночасне надання множини всіляких мережних послуг і передачу по мережі різнотипного трафіку. Для ефективного управління трафіком необхідно мати в своєму розпорядженні відповідні апаратні і програмні засоби, що дозволяють швидко і гнучко надавати користувачеві будь-яку послугу.

Під терміном Traffic Engineering розуміють методи і механізми збалансованого завантаження всіх ресурсів мережі за рахунок раціонального вибору щляху проходження трафіку через мережу. Механізм управління трафіком надає можливість встановлювати явний шлях, по якому передаватимуться потоки даних.

При традиційній маршрутизації IP-трафик маршрутизується за допомогою його передачі від однієї точки призначення до іншої і слідує до пункту призначення по дорозі, що має найменшу сумарну метрику мережного рівня.

Слід зауважити, що за наявності в мережі декількох рівноцінних альтернативних маршрутів трафік ділиться між ними, і навантаження на маршрутизатори і канали зв'язку розподіляється збалансованіше. Але якщо маршрути не є повністю рівноцінними, розподіл трафіку між ними не відбувається.

Ще один істотний недолік традиційних методів маршрутизації трафіку в мережах IP полягає в тому, що шляхи вибираються без врахування поточного завантаження ресурсів мережі. Якщо найкоротший шлях вже переобтяжено, то пакети все одно посилатимуться по цьому шляху. У наявності явна збитковість методів розподілу ресурсів мережі – одні з них працюють з перевантаженням, а інші не використовуються зовсім. Жодні методи QoS дану проблему вирішити не можуть: потрібні якісно інші механізми. Технологія управління трафіком – досить ефективний механізм використання ресурсів мережі.

Основним інструментом вибору і встановлення маршрутів в NGN сьогодні є технологія MPLS. Вона застосовує і розвиває концепцію віртуальних каналів в мережах X.25, Frame Relay і ATM, об'єднуючи її з технікою вибору доріг на основі інформації про топологію і поточне завантаження мережі, що отримується за допомогою протоколів маршрутизації мереж IP.

Для вирішення задач управління трафіком технологія MPLS використовує розширення протоколів маршрутизації, що працюють на основі алгоритму стану зв'язків. Сьогодні такі розширення стандартизовано для протоколів OSPF і IS-IS. Дані протоколи, на відміну від дистанційно-векторних протоколів, до яких відноситься, наприклад, RIP, дають маршрутизатору повну топологічну інформацію про мережу. Їх оголошення містять інформацію про маршрутизатори і мережі, а також про фізичні зв'язки між ними. Кожен зв'язок характеризується поточним станом працездатності і метрикою, як яка використовується величина, зворотна пропускній спроможності каналу.

Для вирішення завдання управління трафіком в протоколи OSPF і IS-IS включені нові типи оголошень для поширення по мережі інформації про номінальну і незарезервовану пропускну спроможність кожного зв'язку. Таким чином, ребра результуючого графа мережі, що створюється в топологічній базі кожного маршрутизатора, будуть маркіровані цими двома додатковими параметрами (рис. 4.18).

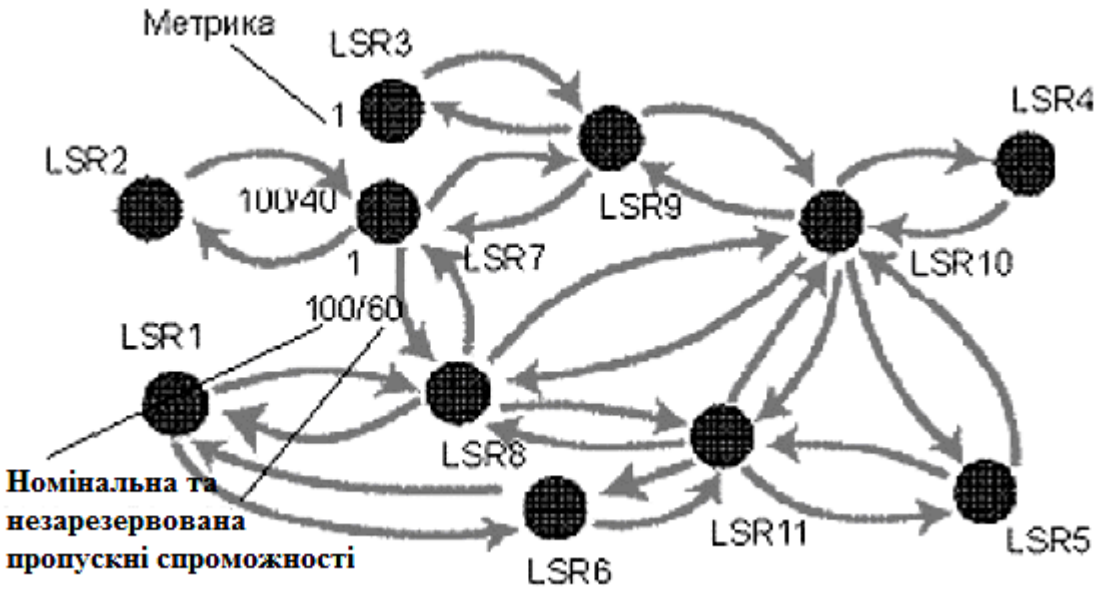


Рис. 4.18 – Граф мережі

З врахуванням графа мережі, а також параметрів потоків, для яких потрібно визначити шляхи управління трафіком, маршрутизатор може знайти раціональне рішення, що задовольняє, наприклад, одному з сформульованих вище обмежень на коефіцієнти використання ресурсів мережі, забезпечивши тим самим її збалансоване завантаження. Для спрощення завдання оптимізації вибір шляхів для деякого набору потоків може здійснюватися по черзі, при цьому як обмеження виступає сумарне завантаження кожного ресурсу мережі. Зазвичай вважається, що внутрішньої продуктивності маршрутизатора вистачає (в середньому) для обслуговування будь-якого трафіку, який здатні прийняти інтерфейси маршрутизатора. Тому в якості обмеження виступають лише максимально допустимі значення коефіцієнтів завантаження каналів зв'язки, що встановлюються індивідуально або в цілому. Рішення задачі визначення маршруту з врахуванням обмежень отримало назву маршрутизації, що базується на обмеженнях (Constrained-based Routing), а протокол OSPF з відповідними розширеннями – Constrained SPF, або CSPF.

Зрозуміло, що пошук маршрутів по черзі знижує якість рішення – при одночасному розгляді всіх потоків можна знайти раціональніше завантаження ресурсів. У прикладі, показаному на рис. 4.19, обмеженням є максимально допустиме значення коефіцієнта використання ресурсів, рівне 0,65.

У варіанті 1 рішення було знайдено при черговості розгляду потоків 1 → 2 → 3. Для першого потоку було обрано маршрут A-B-C, оскільки в цьому випадку він, з одного боку, задовольняє обмеженню (всі ресурси уздовж шляху – канали A-B, A-C і відповідні інтерфейси маршрутизаторів виявляються завантаженими на 0,5/1,5 = 0,33), а з іншої – має мінімальну метрику (65 + 65 = 130). Для другого потоку також було обрано маршрут A-B-C, оскільки і в цьому випадку обмеження задовольняється –

результуючий коефіцієнт використання виявляється рівним (0,5 + 0,4) /1,5 = 0,6. Третій потік прямує за маршрутом A-D-E-C і завантажує ресурси каналів A-D, D-E і E-C на 0,.

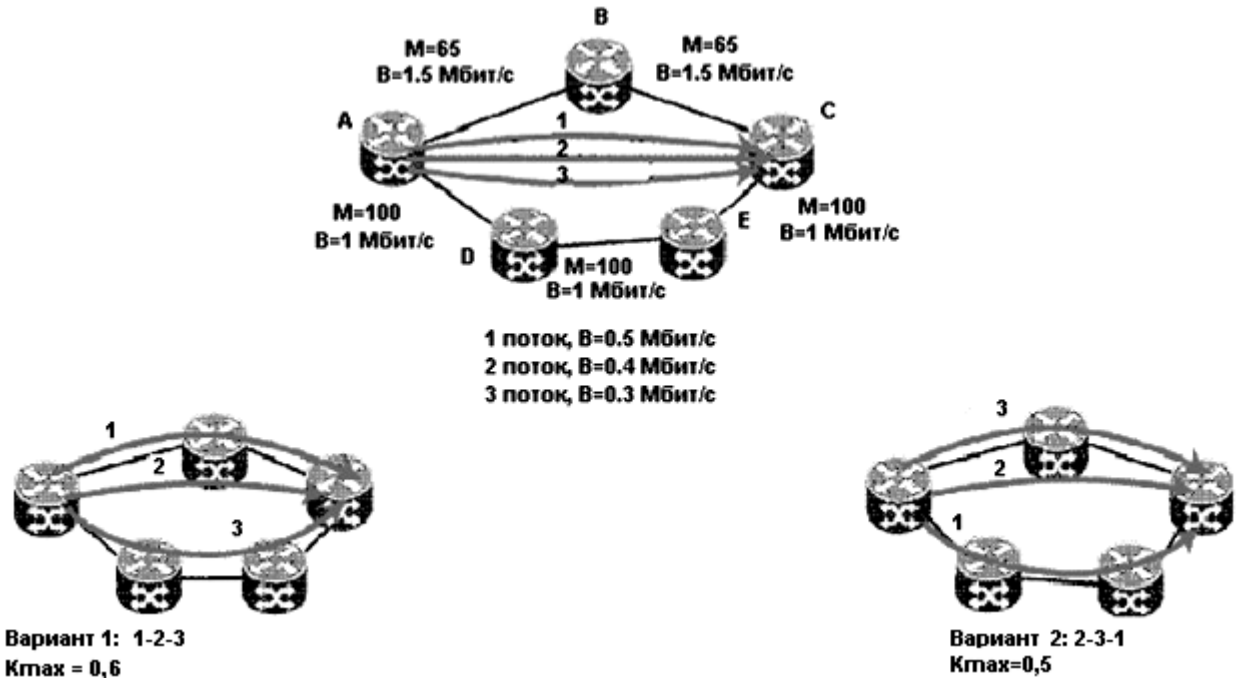


Рис. 4.19 – Варіанти завантаження ресурсів

Перше рішення можна назвати задовільним, оскільки коефіцієнт використання будь-якого ресурсу в мережі не перевищує 0,6.

Проте існує кращий спосіб, представлений у варіанті 2. Тут по верхньому шляху A-B-C були направлені потоки 2 і 3, а потік 1 – по нижньому шляху A-D-E-C. Ресурси верхнього маршруту виявляються завантажені на 0,46, а нижнього – на 0,5, тобто в наявності більш рівномірне завантаження ресурсів, а максимальний коефіцієнт використання по всіх ресурсах мережі не перевищує 0,5.

У технології управління трафіком MPLS інформація про знайдений раціональний маршрут використовується повністю – тобто запам'ятовується не лише перший транзитний вузол, як в основному режимі маршрутизації IP, а всі проміжні вузли маршруту разом з початковим і кінцевим, тобто маршрутизація проводиться від джерела. Тому достатньо, аби пошуком маршруту займалися лише LSR, а внутрішні – лише поставляли їм інформацію про поточний стан мережі, яка необхідна для прийняття рішень. Такий підхід має декілька переваг в порівнянні з розподіленою моделлю пошуку маршруту, що лежить в основі стандартних протоколів маршрутизації IP:

- він дозволяє використовувати "зовнішні" рішення, коли щляхи знаходяться якою-небудь системою оптимізації мережі в автономному режимі, а потім прокладаються в мережі;
- кожен з пограничних LSR може працювати за власною версією алгоритму, тоді як при розподіленому пошуку на всіх LSR

необхідний ідентичний алгоритм, що ускладнює побудову мережі з устаткуванням різних виробників;
- такий підхід розвантажує внутрішні LSR від роботи по пошуку маршрутів.

Після знаходження маршруту незалежно від того, знайдений він був пограничним LSR або зовнішньою системою, його необхідно встановити. Для цього в MPLS TE використовується спеціальний протокол сигналізації, який уміє поширювати по мережі інформацію про явний (explicit) маршрут. Сьогодні для управління трафіком в MPLS визначено два таких протоколу: RSVP-TE і CR-LDP.

При встановленні нового маршруту в повідомленні сигналізації разом з послідовністю адрес маршруту вказується також і резервована пропускна спроможність. Кожен LSR, отримавши таке повідомлення, віднімає запрошувану пропускну спроможність з пулу вільної пропускної спроможності відповідного інтерфейсу, а потім оголошує залишок в повідомленнях протоколу маршрутизації.

4.7.1 Використання тунелів для VPN

Протоколи захищеного каналу, як правило, використовують в своїй роботі механізм тунелювання. За допомогою даної методики пакети даних транслюються через загальнодоступну мережу як по звичайному двоточковому з'єднанню. Між кожною парою "відправник – одержувач даних" встановлюється своєрідний тунель – безпечне логічне з'єднання, що дозволяє інкапсулювати дані одного протоколу в пакети іншого.

Технологія тунелювання дозволяє зашифрувати вихідний пакет цілком, разом із заголовком, а не лише його поле даних. Такий зашифрований пакет поміщається в інший пакет з відкритим заголовком. Цей заголовок використовують для транспортування даних на ділянці загальної мережі. У граничній точці захищеного каналу витягується зашифрований заголовок, який використовуватиметься для подальшої передачі пакету. Як правило, тунель створюється лише на ділянці мережі загального користування, де існує загроза порушення конфіденційності і цілісності даних. Окрім захисту передаваної інформації, механізм тунелювання використовують для забезпечення цілісності і аутентичності. При цьому захист потоку реалізується більш повно.

Тунелювання застосовується також і для узгодження різних транспортних технологій, якщо дані одного протоколу транспортного рівня необхідно передати через транзитну мережу з іншим транспортним протоколом. Слід зазначити, що процес тунелювання не залежить від того, з якою метою він застосовується. Сам по собі механізм тунелювання не захищає дані від несанкціонованого доступу або від спотворень, він лише створює передумови для захисту всіх полів вихідного пакету. Для забезпечення секретності

передаваних даних пакети на транспортному рівні шифруються і передаються по транзитній мережі.

Тунелі MPLS дозволяють передавати дані будь-якого протоколу вищестоящого рівня (наприклад IP, IPX, кадри Frame Relay, вічка ATM), оскільки вміст пакетів уздовж всього маршруту прямування пакету залишається незмінним, міняються лише мітки. На відміну від них, тунелі IPSec підтримують передачу даних лише протоколу IP, а протоколи PPTP і L2TP дозволяють обмінюватися даними за протоколами IP, IPX або Net BEUI. Безпека передачі даних в MPLS забезпечується за рахунок певної мережної політики, що забороняє приймати пакети, забезпечені мітками, і маршрутну інформацію VPN-IP від неперевірених джерел. Вона може бути підвищена використанням стандартних засобів аутентифікації і шифрування (наприклад шифрування IPSec). Для безпечної передачі даних в протокол IP Security включені певні процедури шифрування IP-пакетів, аутентифікації, забезпечення захисту і цілісності даних при транспортуванні, внаслідок чого тунелі IPSec забезпечують надійну доставку інформаційного трафіку. Протокол L2TP підтримує процедури аутентифікації і тунелювання інформаційного потоку, а PPTP окрім даних функцій забезпечений і функціями шифрування. Вживання міток MPLS дозволяє реалізувати прискорене просування пакетів по мережі провайдера. Транспорт MPLS не прочитує заголовки пакетів, що транспортуються, тому використовувана в цих пакетах адресація може носити приватний характер. Вміст пакетів не прочитується і при передачі IP-пакетів по протоколах IPSec, PPTP і L2TP. Проте, на відміну від MPLS, традиційні протоколи тунелювання для транспортування IP-пакетів використовують традиційну IP-маршрутизацію.

При виборі маршруту дотримання пакету в MPLS враховуються різні параметри, що роблять вплив на вибір маршруту. Спільна робота технології багатопротокольної комутації і механізмів Traffic Engineering дозволяє для кожного тунелю LSP надати необхідний рівень якості обслуговування за рахунок процедури резервування ресурсів на кожному маршрутизаторі уздовж маршруту дотримання пакету. Окрім цього, з'являється можливість відстежувати дійсний маршрут, що проходить через сформований тунель, можливість діагностики і адміністративного контролю тунелів LSP.

Різні тунелі, відповідно до необхідного рівня QoS між двома точками підтримує і протокол L2TP. Технологія VPN IPSec не підтримує параметрів якості обслуговування встановленого з'єднання, а протокол PPTP підтримує єдиний тунель між двома точками. Не можна не відзначити і той факт, що весь трафік при використанні традиційних IP-тунелів слідує до адресата уздовж одного і того ж маршруту. Технологія MPLS дозволяє контролювати потоки, що передаються по множині всіх наявних шляхів до адресата. Варто відзначити, що жодна з даних технологій не підтримує багатоадресну розсилку, але для MPLS вона знаходиться в розробці. MPLS VPN може бути створена для підтримки критично важливих застосувань на цілодобовій основі. В цьому випадку провайдер послуг визначає фіксований маршрут на термін контракту з користувачем. У випадках збою або відсутності пропускної спроможності пріоритет віддається важливішим потокам (з вищим пріоритетом). Одна з

функцій MPLS - об'єднання віртуальних каналів, коли декілька тунелів MPLS об'єднуються для створення єдиного тунелю. Така структура поширює VPN на базі MPLS в мережі оператора на мережу усередині офісу і прямо до сервера або клієнта. При подібному розширенні VPN операторові може бути надана відповідальність по управлінню для забезпечення безперервного контролю за CoS з кінця в кінець.

4.8 Якість обслуговування в мережі MPLS

Забезпечення функцій QoS – це важливий компонент технології MPLS. В мережі MPLS інформація пов'язана з функціями QoS передається в поле CoS заголовка MPLS-метки.

Виконання функцій QoS в мережі MPLS досягається так само, як і в мережі IP, за допомогою виконання двох головних логічних кроків, які показані в таблиці 4.4, і використовує такі ж функції QoS.

Таблиця 4.4 - Виконання функцій QoS в мережі MPLS

№	Місце вживання	Відповідні функції QoS	Дія QoS
1	Маршрутизатор на вході в MPLS-домен (граничний маршрутизатор)	Узгодження швидкості доступу (Committed Access Rate - CAR)	Варіант 1. Механізм CAR обмежує трафік на вхідному маршрутизаторі для всього IP-трафіка, що поступає в MPLS-домен. Він встановлює для трафіку значення IP- пріоритету виходячи з профілю трафіку і існуючих політик. Значення поля IP-пріоритету копіюється в полі MPLS CoS. Варіант 2. Механізм CAR обмежує трафік на вхідному маршрутизаторі для всього IP- трафіку, що поступає в MPLS-домен. Для трафіку встановлюється значення поля MPLS CoS виходячи з профілю трафіку і існуючого контракту. На відміну від варіанту 1, значення пріоритету в IP- заголовку залишається незмінним
	Вся мережа MPLS	Зважений алгоритм рівномірного обслуговування черг (Weighted Fair Queuing - WFQ). Зважений алгоритм довільного раннього виявлення (Weighted Random Early Detection WRED)	Диференціація трафіку в MPLS-магістралі на підставі значення поля MPLS CoS за допомогою функцій IP QoS WFQ і WRED.

MPLS використовує функції IP QoS для реалізації різних рівнів обслуговування трафіку, який передається в мережі MPLS. Єдина відмінність полягає в тому, що MPLS QoS базується на бітах CoS мітки MPLS, тоді як IP QoS базується на значенні поля пріоритету в заголовку пакета IP.

4.8.1 Реалізація служби IntServ в мережі MPLS

Механізм інтегрованих служб IntServ забезпечує повнофункціональний механізм QoS за рахунок забезпечення наскрізної сигналізації, підтримки стану (для кожного потоку RSVP) і управління доступом для кожного мережного елементу.

Практично QoS реалізується за допомогою різних механізмів. У якості протоколу сигналізації IntServ використовується протокол резервування ресурсів (Resource Reservation Protocol - RSVP), а в якості механізмів завдання правил і формування потоків – параметр погодженої швидкості передачі (Committed Access Rate - CAR), протокол загального обмеження потоку даних (Generic Traffic Shaping – GTS).

Протокол RSVP може виконувати резервування для об'єднаних (інтегрованих, агрегованих) потоків даних. Дана функція утворює основу реалізації протоколу RSVP в MPLS, згідно якої пакети, що належать до зарезервованого потоку, можуть розглядатися як пакети одного класу еквівалентності при пересилці (Forwarding Equivalence Class - FEC). При цьому можуть бути створені таблиці прив'язки міток до комплексів класів еквівалентності FEC. Після цього мітки можуть бути поширені по мережі з використанням протоколу LDP або розширених протоколів маршрутизації.

Комутація MPLS може бути активізована на пристрої LSR шляхом логічного скріплення міток з потоками, для яких створено RSVP-резервування. Пакети, для яких було зроблено RSVP-резервування, можуть розглядатися як класи FEC. Кожен клас FEC ідентифікується своєю міткою. Прив'язка міток і потоки RSVP мають бути поширена між LSR-пристроями.

Як показано на рис. 4.20, після отримання RSVP-повідомлення PATH, вузол відповідає стандартним повідомленням RESV. Пристрій LSR3 отримує повідомлення RESV, виділяє мітку з пулу вільних міток і відправляє пристрою LSR2 повідомлення, в якому міститься об'єкт LABEL (тобто мітка) і значення мітки (7). Він також заносить в свою ба зу LFIB мітку 7 в якості вихідної мітки. Після цього пристрій виділяє нову мітку (3) для використання її в якості вхідної мітки, яка передається наступному на маршруті пристрою LSR1. У міру того як повідомлення RESV з об'єктом LABEL переміщається по маршруту, уздовж маршруту RSVP створюється маршрут LSP і кожен LSR-пристрій може логічно пов'язати ресурси QoS з маршрутом LSP.

У робочому режимі, коли пристрій LSR2 отримує від пристрою LSR1 пакет із значенням мітки 3, він може проглянути базу LFIB і знайти там інформацію про всі QoS-механізми, пов'язані з цим пакетом, такі, наприклад, як IP- черговість. При цьому не потребується проведення аналізу заголовків протоколу IP і транспортного протоколу.

На рис. 4.20 пристрій LSR1 представлено логічні зв'язки всіх пакетів конкретного класу FEC до призначеного їм певного LSP-маршруту. Наприклад, всі пакети, призначені певному префіксу пункту призначення, можуть бути направлені на конкретний маршрут LSP.

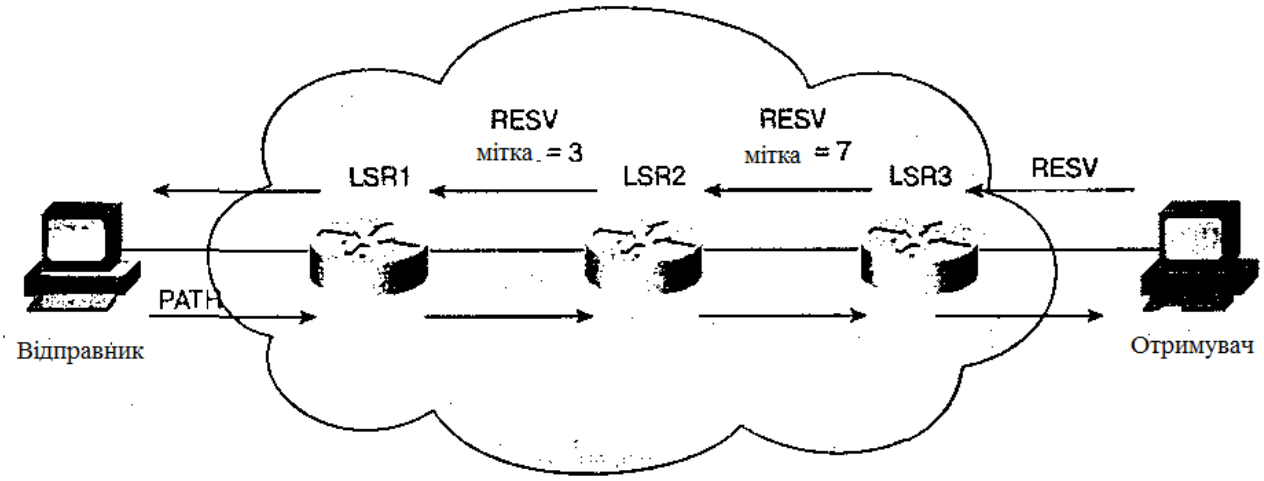


Рис. 4.20 – Обмін повідомленнями PATH і RESV в мережі MPLS

Таким чином один маршрут LSP може забезпечити гарантії якості обслуговування QoS великій кількості потоків даних.

4.8.2 MPLS-реализация функцій DiffServ

LSR-пристрої мережі MPLS не аналізують вміст IP-заголовка і значення його поля DSCP, як вимагає механізм DiffServ. Це означає, що рішення щодо відповідної політики PHB має отримуватися із значення мітки. Проміжний заголовок MPLS має 3-бітове поле Exp. Спочатку воно розглядалося як експериментальне. Дане поле може містити до восьми значень і використовується в комутації MPLS для підтримки до 8 класів DiffServ. Як показано на рис. 4.21, біти пріоритету відкидання пакетів або перших 3 біта поля DSCP на межі мережі копіюються в полі Exp заголовка MPLS. Кожний LSR- пристрій на маршруті LSP перетворить біти поля Exp в значення, необхідне для PHB. Провайдер служби може також встановити інше значення CoS пакету MPLS, визначене при наданні служби. Дана функція дозволяє провайдерові встановлювати поле Exp MPLS замість того, щоб переписувати значення призначеного для користувача поля IP-пріоритету для визначення політики відкидання пакетів, що надає можливість зберегти IP-заголовок в первинному стані і використовувати його надалі.

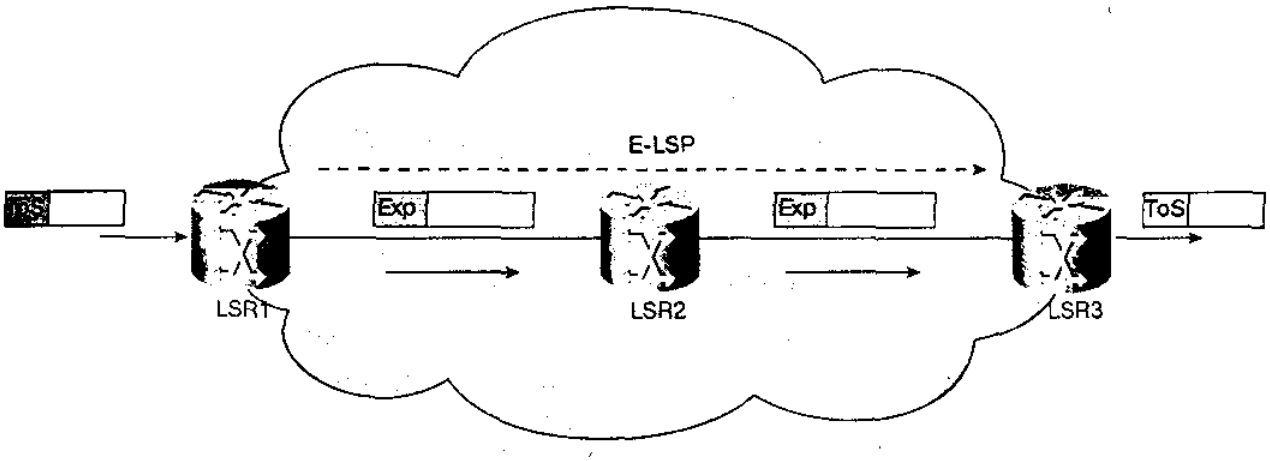


Рис. 4.21 – Маршрути E-LSP в мережі MPLS

При просуванні пакету по MPLS-магістралі сконфігурований користувачем клас CoS не змінюється. Маршрути LSP, створені таким чином, називають маршрутами E-LSP або EXP-LSP. Маршрути E-LSP можуть підтримувати до восьми класів PHB на кожному LSP-маршруті.

Контрольні запитання

1. Поясніть, за рахунок чого прискорюється процес маршрутизації в мережах MPLS?
2. Поясніть розташування рівнів архітектури MPLS відносно ієрархії моделі OSI
3. Назвіть основні функції площини пересилки даних MPLS
4. Назвіть основні функції площини управління MPLS
5. Що таке клас еквівалентності пересилки FEC?
6. За якими ознаками обираються класи FEC?
7. Чому дорівнює максимальне значення ідентифікатора мітки?
8. Якщо бітове поле стека мітки *S=0*, що це означає ?
9. Які правила інкапсуляції міток при використанні технології MPLS разом з асинхронним режимом передавання ATM ?
10. Які правила інкапсуляції міток при використанні технології MPLS разом з технологією Ethernet ?
11. Проведить порівняння традиційної IP-маршрутизації з маршрутизацією MPLS
12. Для чого використовується інформаційна база пересилки LFIB ?
13. Назвіть механізми встановлення LSP-маршрутів
14. Визначте загальні принципи функціонування протоколу LDP

Розділ 5. Рівень доступу. Мережа LTE як мобільний сегмент NGN.

5.1. Загальні принципи переходу мереж безпроводового зв'язку до NGN

У різних джерелах ми зустрічаємося з поняттями мереж безпроводового зв'язку наступного покоління (Next Generation Wireless Network, NGN), систем «після 3G» (Beyond 3G, B3G) і систем 4G. Єдиного трактування відмінності між ними немає. Системи «після 3G» часто фігурують в документах, що відображають бачення ITU і світового дослідницького форуму по безпроводовому зв'язку (Wireless World Research Forum, WWRF), тоді як термін 4G зустрічається в публікаціях IEEE (Інституту інженерів електроніки і електротехніки, Institute of Electrical and Electronics Engineers). Вочевидь, з часом поняття «Після 3G» вийде з вживання, а ті або інші системи, по накопиченню достатнього числа технологічних ознак, відноситимуть до третього або до четвертого покоління (табл. 5.1).

В цілому, те, що об'єднує всі точки зору відносно 4G, зводиться до двох нижченаведених положень:

Таблиця 5.1-Стисла історія розвитку технологій мобільного зв'язку

Покоління	1G	2G	2.5G	3G	4G
Види послуг	Аналогова мова, передача даних до 9.6 Кбіт/с	Цифрова мова, SMS	Високо-швидкісна пакетна передача	Широкопо-лосна передача даних (до 2 Мбіт/с)	Передача даних і мультимедіа на базі IP-протокола (до сотень Мбіт/с)
Стандарти	AMPS, TACS, NMT і ін.	TDMA, GSM, CDMA, PDC	GPRS, EDGE, IXRTT	WCDMA, CDMA2000	Єдиний стандарт
Швидкість передачі	1.9 Кбіт/с	14.4 Кбіт/с	384 Кбіт/с	2 Мбіт/с	200 Мбіт/с
Метод мультиплексування	FDMA	TDMA, CDMA	TDMA, CDMA	CDMA	CDMA, OFDMA
Базова мережа	PSTN	PSTN	PSTN, пакетна мережа	Пакетна мережа	Internet

Системи 4G - це нові системи безпроводового зв'язку з високою спектральною ефективністю і радіоінтерфейсами, що підтримують обмін даними з піковою швидкістю 100 Мбіт/с в мобільному варіанті з глобальним

покриттям, і до 1 Гбіт/с - для обмеженої зони і для об'єктів з малою рухливістю;

Для систем 4G буде характерною максимальна інтеграція різних безпроводових платформ, що мають відкриту архітектуру [4].

Принципи відкритої безпроводової архітектури (open wireless architecture - OWA) можна сформулювати таким чином:

- інтеграція розвиваючихся та новостворюваних систем безпроводового доступу, стільникового і проводового зв'язку на єдиній реконфігурованій платформі з метою забезпечення гнучкості і різноманіття надання послуг;
- розробка конвергентної широкосмугової платформи на базі відкритої безпроводової архітектури, яка дозволяє оптимізувати процес надання послуг для різних категорій користувачів, що приведе до появи єдиного промислового стандарту (сервісне середовище існуючих мобільних систем: GPRS, cdma2000, UMTS визначається їх базовою мережею, не дозволяючи надавати послуги за її межами);
- інтеграція радіоінтерфейсів на базі універсального терміналу з унікальним IP-адресом, що функціонує в середовищі безпроводового доступу і виконує роль основного персонального комунікаційного засобу.

Концепція розвитку мобільних мереж NGN з точки зору провідних організацій в області стандартизації безпроводових мереж (ITU-R, IEEE) передбачає:

- наявність широкого набору послуг, включаючи мобільне мультимедіа з опціями QoS. Розвиток таких технологій, як багатопозиційні антенні системи (MIMO), методи множинного доступу і модуляції, мережні IP-технології;
- розгортання спектральне ефективних мобільних систем широкосмугового доступу на глобальній основі, заповнення ніші між високошвидкісними послугами мереж безпроводового широкосмугового доступу на базі стандартів серії IEEE 802 і послугами мереж стільникового зв'язку.
- розробка специфікацій радіоінтерфейсу фізичного і MAC-рівнів, що забезпечує взаємодію мобільних широкосмугових систем пакетного доступу в частотних діапазонах, що ліцензуються, нижче 3.5 ГГц, який дозволить підтримувати пікову швидкість передачі даних не менше 1Мбіт/с для користувачів, що переміщаються з швидкістю до 250 км/ч; забезпечить радіопокриття в зонах (сотах), радіус яких порівнянний з радіусом покриття в мережах WMAN; забезпечить спектральну ефективність, швидкість передачі інформації і число одночасно підтримуваних з'єднань істотно більші, ніж існуючі системи мобільного зв'язку третього покоління.

Основною характеристикою безпроводового зв'язку наступного покоління є архітектурна інтеграція на основі протоколу IP.

Для систем безпроводового зв'язку наступного покоління буде характерним співіснування і взаємодоповнення різних технологій радіодоступу, які забезпечать інтегровані безшовні послуги на основі єдиної

опорної мережі. Створена багаторівнева архітектура забезпечить гнучке масштабоване середовище доступу до набору послуг. У цьому сенсі на сьогоднішній день IP-протокол як технологія функціональної інтеграції мереж не має альтернативи.

Одна з найбільш оформлених концепцій безпроводових систем покоління 4G шляхом модернізації платформи UMTS міститься на сьогоднішній день в документах Release 8 проекту 3GPP, в рамках програми LTE (Long-Term Evolution- Довготривала Еволюція).

5.2 Принципи побудови і функціонування мереж LTE.

Архітектура мережі LTE розроблена так, щоб забезпечити підтримку пакетного трафіку з так званою “гладкою” (“безшовною”, seamless) мобільністю, мінімальними затримками доставки пакетів і високими показниками якості обслуговування.

Мобільність як функція мережі забезпечується двома її видами: дискретною мобільністю (роумінгом) і безперервною мобільністю (хендовером).

При розробці архітектури мережі LTE були взяті до уваги наступні загальні принципи.

- Логічно розділені транспортні (під) мережі передачі призначених для користувача даних і службової інформації.
- Управління мобільністю абонентів і користувачевих терміналів повністю покладене на мережу радіодоступу.
- Інтерфейси повинні базуватися на логічній моделі блоку, керованого даним інтерфейсом.
- Один фізичний елемент мережі може реалізаційний містити в собі декілька логічних блоків.

5.2.1 Архітектура мережі LTE

Мережа LTE складається з двох найважливіших компонентів: мережі радіодоступу E-UTRAN і базовій мережі SAE (System Architecture Evolution), яка також називається базовою мережею EPC (Evolved Packet Core).

Архітектуру мереж LTE можна назвати “плоскою”, оскільки практично вся мережна взаємодія відбувається між двома вузлами: базовою станцією (БС), яка в технічних специфікаціях називається B-вузлом (B-вузол, NODE-B, eNB) і блоком управління мобільністю (MME, Mobility Management Entity), який, як правило, включає і мережний шлюз (GW, Gateway), тобто мають місце комбіновані блоки MME/GW.

Контролер радіомережі, що грав вельми значну роль в мережах попередніх поколінь, усунений від управління потоком даних (фактично він навіть відсутній

в структурних схемах), а його традиційні функції – управління радіоресурсами, стискання заголовків, шифрування, надійна доставка пакетів і ін. передані безпосередньо БС.

Блок управління мобільністю MME працює лише із службовою інформацією - так званою мережною сигналізацією, так що IP-пакети, що містять призначену для користувача інформацію, через нього не проходять. Головною функцією MME є управління терміналами користувачів, що знаходяться в режимі чекання, включаючи перенаправлення і виконання викликів, авторизацію і аутентифікацію, роумінг і хендовер, встановлення службових і призначених для користувача каналів і так далі.

Серед всіх мережних шлюзів окремо виділені два: обслуговуючий шлюз S-GW (Serving Gateway) і шлюз пакетної мережі P-GW (Packet Data Network Gateway). S-GW функціонує як блок управління локальною мобільністю, приймаючи і пересилаючи пакети даних, що відносяться до БС і обслуговуваним їм терміналам користувача. P-GW є інтерфейсом між набором БС і різними зовнішніми мережами, а також виконує деякі функції IP-мереж, такі, як розподіл адресів, забезпечення призначених для користувача політик, маршрутизація, фільтрація пакетів і ін.

Як і в більшості мереж третього покоління, в основу принципів побудови мережі LTE покладено розділення двох аспектів: фізичній реалізації окремих мережних блоків і формування функціональних зв'язків між ними. При цьому завдання фізичної реалізації вирішуються, виходячи з концепції області (domain), а функціональні зв'язки розглядаються в рамках шару (stratum).

Первинним розділенням на фізичному рівні є розділення архітектури мережі на область користувачевого обладнання (UED, User Equipment Domain) і область мережної інфраструктури (ID, Infrastructure Domain). Остання, у свою чергу, розділяється на мережу радіодоступу (E-UTRAN, Evolved Universal Terrestrial Radio Access Network) і базову пакетну мережу (EPC, Evolved Packet Core).

Обладнання користувача – це сукупність користувачевих терміналів з різними рівнями функціональних можливостей, використовуваних мережними абонентами для доступу до LTE-послуг.

На рис. 5.1 показана узагальнена структура мережі LTE, з якої видно наявність двох шарів функціональних зв'язків: шару радіодоступу (AS, Access Stratum) і зовні шару радіодоступу (NAS, Non-Access Stratum). Показані на рис. 5.1 овали із стрілками позначають точки доступу до послуг.

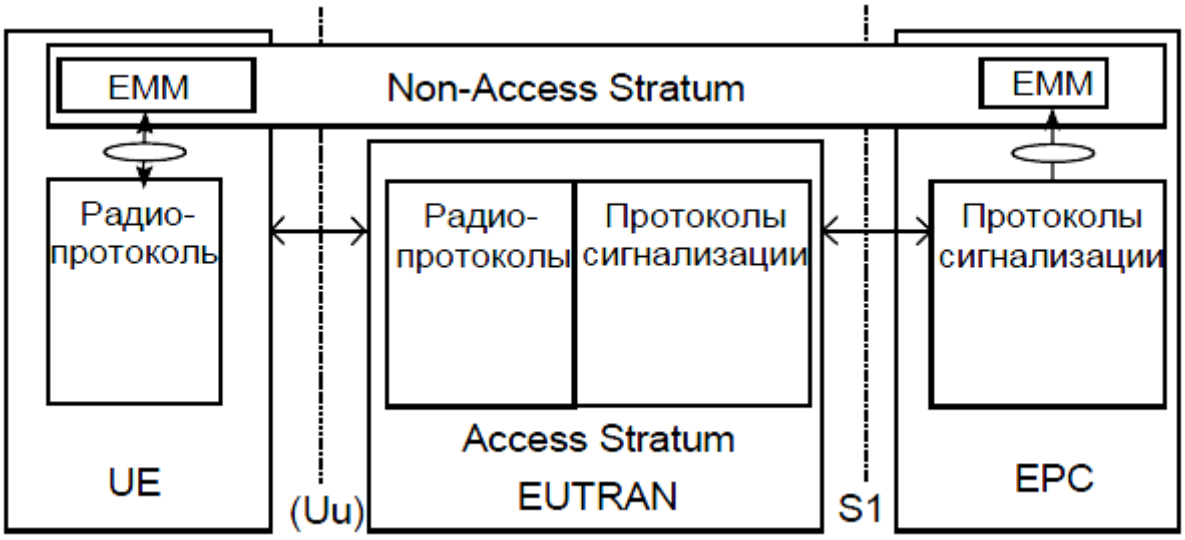


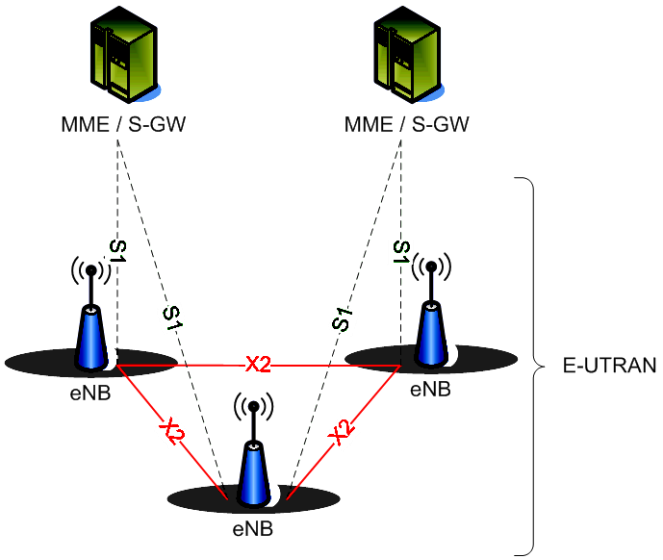
Рис. 5.1 - Узагальнена структура мережі LTE

Стик між областю UE обладнання користувача і областю мережі радіодоступу UTRAN називається Uu-інтерфейсом; стик між областю мережі радіодоступу і областю базової мережі EPC – S1-интерфейсом. Склад і функціонування різних протоколів, що відносяться до інтерфейсів Uu і S1, розділені на дві так звані площини: користувачеву площину (UP, User Plane) і площину управління (CP, Control Plane).

Зовні шару доступу діють механізми управління мобільністю в базовій мережі (EMM, EPC Mobility Management).

В користувачевій площині реалізовані протоколи, що забезпечують передачу даних користувача по радіоканалу. До площини управління відносяться ті протоколи, які в різних аспектах забезпечують з'єднання між терміналом користувача і мережею. Також до цієї площини відносяться протоколи, призначені для прозорої передачі повідомлень, що відносяться до надання різних послуг.

Область мережі радіодоступу логічно розділена на два рівні: рівень радіомережі (RNL, Radio Network Layer) і рівень транспортної мережі (TNL, Transport Network Layer). Взаємодія БС, що входять в область мережі радіодоступу, здійснюється на основі X2-інтерфейса (рис. 5.2). Крім того, має місце транзитне з'єднання між базовими станціями і базовою мережею через блок управління мобільністю (S1-MM-інтерфейс) або обслуговуючий вузол (S1-U-інтерфейс). Таким чином, можна стверджувати, що S1-інтерфейс підтримує множинні стосунки між набором БС і блоками MME/S-GW.



eNB – базові станції; Serving GW – загальний шлюз доступу;
X2 - фізичний інтерфейс між базовими станціями для забезпечення хендовера
LTE-Uu - фізичний інтерфейс користувача;
S1-u - інтерфейс передачі даних користувача
S1-c – службовий інтерфейс MME

Рис. 5.2 - З'єднання функціональних вузлів мережі радіодоступу

Розглянемо призначення функціональних блоків мережі радіодоступу [5].

На БС в мережах LTE покладено виконання наступних функцій:

- Управління радіоресурсами: розподіл радіоканалів, динамічний розподіл ресурсів у висхідних і низхідних напрямах - так звана диспетчеризація ресурсів (scheduling) і ін.
- Стискування заголовків IP-пакетів, шифрування потоку призначених для користувача даних.
- Вибір блоку управління мобільністю при включенні в мережу терміналу користувача за відсутності в того інформації про минуле підключення.
- Маршрутизація в площині користувача пакетів даних у напрямку до обслуговуючого шлюзу.
- Диспетчеризація і передача викличної і мовної інформації, отриманої від MME.
- Диспетчеризація і передача повідомлень PWS (Public Warning System, система тривожного сповіщення), отриманих від MME.
- Вимір і складання відповідних звітів для управління мобільністю і диспетчеризації.

Блок управління мобільністю забезпечує виконання наступних функцій.

- Передача захищеної інформації про точки доступу до послуг і захищене управління точками доступу.
- Передача інформації в базову мережу для управління мобільністю між різними мережами радіодоступу.
- Управління БС, що знаходяться в стані чекання, включаючи перенаправлення викликів.

- Управління списком зон відстежування терміналів користувача.
- Вибір обслуговуючого шлюзу і шлюзу пакетної мережі для мереж радіодоступу різних стандартів.
- Вибір нового блоку управління мобільністю при виконанні хендовера.
- Роумінг.
- Аутентифікація.
- Управління радіоканалом, включаючи установку виділеного каналу.
- Підтримка передачі повідомлень PWS.

Обслуговуючий вузол відповідає за виконання наступних функцій:
- Вибір точки прив'язки локального місця (Local Mobility Anchor) розташування при хендовері.
- Буферизація пакетів даних в низхідному напрямі, призначених для терміналів користувача, що знаходяться в режимі чекання, і ініціалізація процедури запиту послуги.
- Санкціоноване перехоплення інформації користувача.
- Маршрутизація і перенаправлення пакетів даних.
- Маркіровка пакетів транспортного рівня.
- Формування облікових записів користувачів і ідентифікатора класу якості обслуговування для тарифікації.
- Тарифікація абонентів.

Шлюз пакетної мережі забезпечує виконання наступних функцій.
- Фільтрація призначених для користувача пакетів.
- Санкціоноване перехоплення призначеної для користувача інформації.
- Розподіл IP-адресів для термінала користувача.
- Маркіровка пакетів транспортного рівня в низхідному направлінні.
- Тарифікація послуг, їх селекція.

5.2.2 Стеки протоколів

Стек протоколів, що відноситься до призначеної для користувача площини розподілений за наступними рівнями:

- фізичний (PHY) рівень;
- підрівень управління доступом до середовища MAC (Medium Access Control);
- підрівень управління радіоканалом RLC (Radio Link Control);
- рівень протоколу конвергенції (злиття) пакетних даних PDCP (Packet Data Convergence Protocol).
- мережний рівень IP;

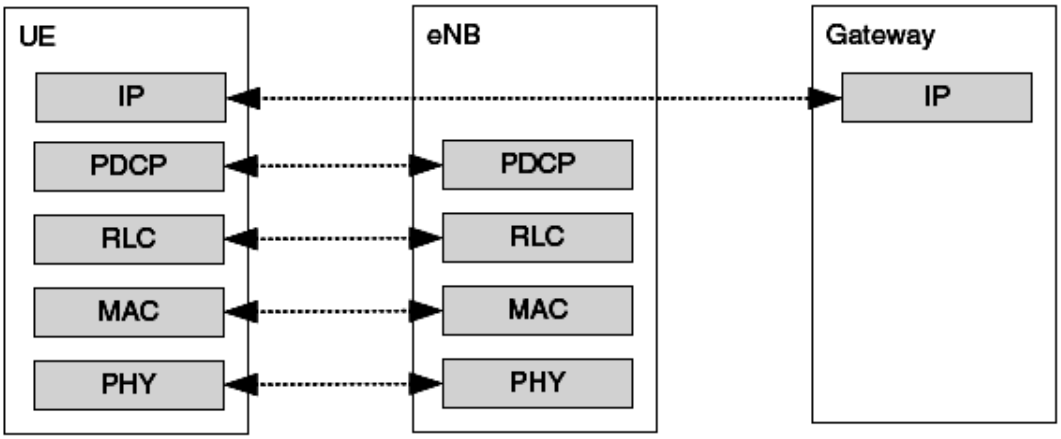


Рис. 5.3 Стек протоколів в площині користувача

Стек протоколів, що відноситься до площини управління розподілений по наступних рівнях:

- фізичний (PHY) рівень;
- підрівень управління доступом до середовища MAC (Medium Access Control);
- підрівень управління радіоканалом RLC (Radio Link Control);
- рівень протоколу конвергенції (злиття) пакетних даних PDCP (Packet Data Convergence Protocol).
- рівень управління радіоресурсами RRC (Radio Resource Control);
- рівень протоколу, що функціонує зовні шару доступу (NAS-протокол).

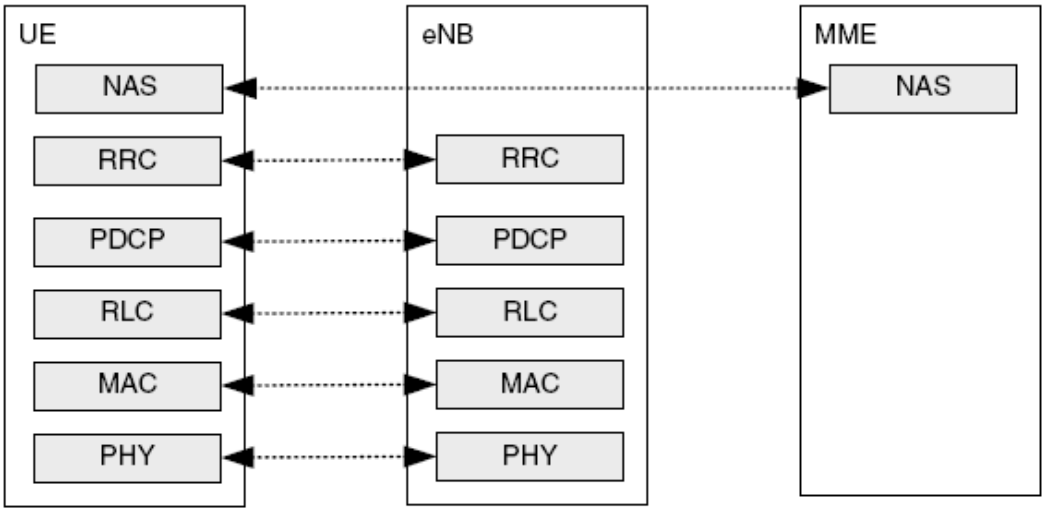


Рис. 5.4. Стек протоколів в площині управління

Як видно з рис. 5.3 і 5.4, на підрівнях MAC і RLC в призначеній для користувача площині виконуються такі ж функції, що і в площині управління.

На фізичному рівні, званому також Рівнем 1 (L1, Layer 1) забезпечуються наступні функції.

- Виявлення помилок в транспортному каналі і індикація про це на вищі рівні.
- Перешкодостійке кодування і декодування даних в транспортному каналі.
- Гібридні запити на повторну пересилку пакетів даних (комбінацію методів виявлення помилок з повторною передачею пакетів).
- Енергетичне вирівнювання фізичних каналів за допомогою вагових множників.
- Модуляція/демодуляція фізичних каналів.
- Частотна і часова синхронізація.
- Вимір радіочастотних характеристик і індикація про це на вищі рівні.
- Рознесена передача і паралельна антенна обробка (методи MIMO, Multiple Input Multiple Output).
- Формування діаграми спрямованості.
- Радіочастотна обробка сигналів.

Точки доступу до послуг між фізичним рівнем і MAC-рівнем забезпечуються транспортними каналами, а між MAC-рівнем і RLC-рівнем - логічними каналами.

На MAC-підрівні канального рівня забезпечується виконання наступних основних функцій:

- Мультиплексування пакетів послуг (SDU, Service Data Unit), що відносяться до одного або декількох логічних каналів, в транспортні блоки транспортних каналів і виконання зворотних функцій.
- Диспетчеризація складання звітів.
- Виправлення помилок через запити на повторну передачу.
- Управління пріоритетом між логічними каналами.
- Ідентифікація послуг мультимедійного мовлення (MBMS, Multimedia Broadcast Multicast Service).
- Вибір транспортного формату.
- Вирівнювання вмісту пакетів даних.

Передача даних на RLC-підрівні може відбуватися в двох режимах: з підтвердженням (AM, Acknowledge Mode) або без підтвердження (UM, Unacknowledge Mode). Режим без підтвердження, при його можливому використанні в радіоканалі, допускає деяку втрату пакетів даних. У режимі з підтвердженням використовується механізм автоматичних запитів на повторну передачу втрачених пакетів.

На RLC-підрівень канального рівня покладені наступні функції.

- Передача пакетів даних на вищий рівень.

- Виправлення помилок через запити на повторну передачу (лише у режимі з підтвердженням).
- Конкатенація (зчеплення), сегментація і повторна збірка пакетів послуг.
- Повторна сегментація пакетів даних (лише у режимі з підтвердженням).
- Зміна порядку прямування пакетів даних.
- Функціонування протоколу виявлення помилок (лише у режимі з підтвердженням).
- Відкидання спотворених пакетів послуг.
- Повторна установка з'єднання на рівні RLC.

Функції PDCP- підрівня канального рівня:

- Стискання/відновлення заголовків за протоколом ROHC (Robust Header Compression).
- Передача користувачевих даних.
- Послідовна доставка пакетів даних більш високого рівня (у режимі з підтвердженням).
- Повторна передача пакетів послуг при хендовері (у режимі з підтвердженням).
- Шифрування/дешифрування.
- Відкидання спотворених пакетів послуг у висхідному напрямі.
- Передача управляючої інформації.

Основні послуги і функції RRC-підрівня включають:

- Здійснення викликів.
- Установка, регулювання і розрив з'єднання на RRC-підрівні між терміналом користувача і мережею.
- Функції захисту інформації, включаючи управління ключами шифрування.
- Установка, конфігурація, регулювання і зняття наскрізного радіоканалу.
- Функції управління мобільністю.
- Підтвердження послуг мультимедійного мовлення.
- Управління якістю обслуговування.
- Складання звітів про вимір параметрів, що відносяться до терміналу користувача.
- Прямий обмін повідомленнями між терміналом користувача і мережною областю зовні шару доступу.

5.2.3 Наскрізний канал (end-to-end bearer)

В мережах LTE (також, як і в мережах UMTS) вводиться поняття наскрізного каналу (end-to-end bearer) між двома кінцевими точками: або між двома користувачами, або, наприклад, між призначеним

для користувача терміналом і яким-небудь Інтернет - сервером. Відповідно цьому, виникають поняття частини наскрізного каналу – на різних рівнях і в різних мережних вузлах: радіоканал (radio bearer), зовнішній канал (external bearer) і ін. Зокрема, має місце поняття каналу, що переносить ряд параметрів якості обслуговування, що встановлюється між терміналами користувача і шлюзом пакетної мережі (рис. 5.5); у LTE-специфікаціях такий канал називається EPS-канал (EPS bearer, EPS - Evolved Packet System, виділена пакетна система). Кожен IP-поток, наприклад, голосовий трафік, передаваний за допомогою IP-протокола (VoIP), пов'язаний з індивідуальним EPS-каналом, і, відповідно до цього, мережа здатна встановлювати різним абонентам різні пріоритети. Коли IP-пакет приходить ззовні (зовнішня IP-сеть, Інтернет), він класифікується обслуговуючим вузлом за якістю обслуговування на основі передвстановлених параметрів, відображується у відповідний EPS-канал і далі передається по радіоканалу між БС і терміналами користувача. Таким чином, існує взаємно-однозначна відповідність між EPS-каналом і радіоканалом.

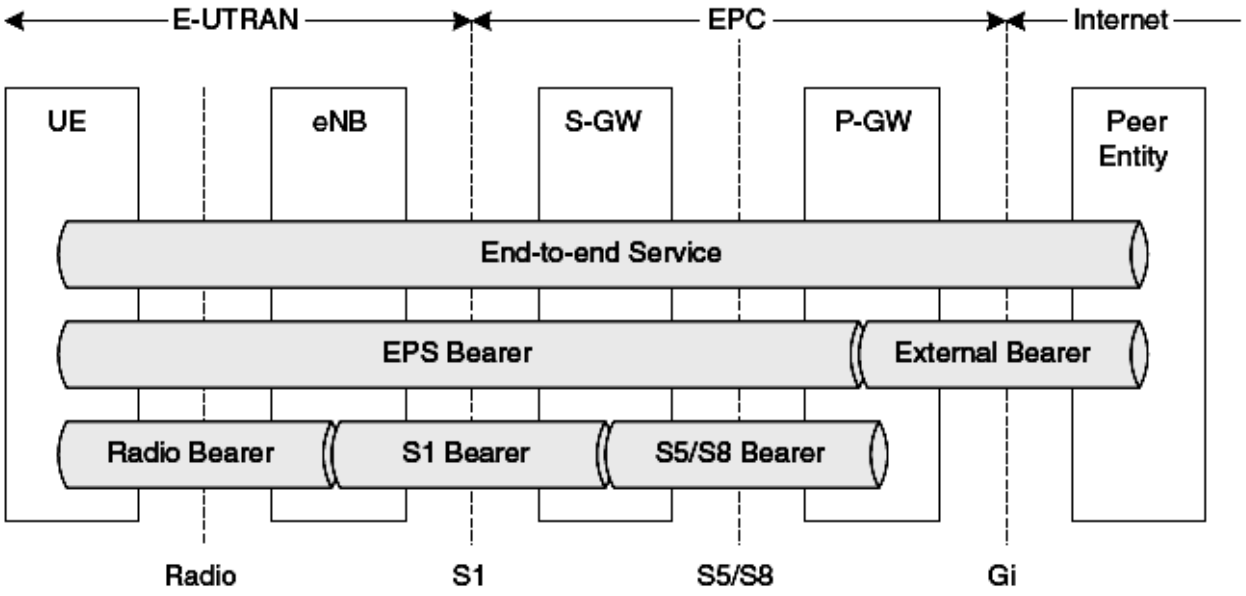


Рис. 5.5 - Архітектура наскрізного каналу

5.2.4 Структура каналів на радіоділянці

E-UTRAN розроблений як частина мережі All-IP, тому мережа доступу LTE більше не має елементів, заснованих на комутації каналів. Широкомовні і загальні канали, специфіковані в попередніх версіях 3GPP (HSDPA, HSUPA, MBMS), також використовуються в LTE. Стек протоколів сигналізації, який використовується в LTE, заснований на стандартній семирівневій моделі OSI. На третьому рівні представлені логічні канали, які надають послуги протоколам верхнього рівня, що відповідають за реалізацію послуг і роботу застосувань. Потім логічні

канали співставляються з транспортними каналами на другому рівні, які управляють потоками даних (повторними передачами, контролем помилок, пріоритизацією) [6].

На другому рівні функціонують протоколи RLC, PDCP і MAC. На фізичному рівні транспортні канали співвідносяться з фізичними, використовуючими радіоінтерфейс.

Логічні канали мережного рівня надають свої функції верхнім рівням стека протоколів і специфіковані в термінах сервісів верхнього рівня, які вони підтримують. Кожен логічний канал визначається типом інформації, яку він переносить.

У загальному випадку, логічні канали LTE розбиті на дві групи:

• логічні канали управління (для перенесення інформації рівня управління);

• користувачеві логічні канали (для перенесення призначеної для користувача інформації).

Користувачеві канали (traffic channels):

• DTCH - Dedicated Traffic Channel - індивідуальний користувачувий канал з конфігурацією точка-точка, привласнений для терміналу користувача.

• MTCH - Multicast Traffic Channel - однонаправлений канал від eNB до терміналу користувача. Використовується тими терміналами, які отримують MBMS (Multimedia Broadcast Multicast Service) - широкомовні і багатоадресні послуги.

Канали управління (control channels):

• BCCH - Broadcast Control Channel - однонаправлений канал для передачі широкомовної інформації управління;

• PCCH - Paging Control Channel - однонаправлений канал, який переносить інформацію для пошуку абонента. Цей канал використовується, якщо мережа не знає соти, в якій в даний момент знаходиться абонент;

• CCCH - Common Control Channel - цей канал призначений для запиту доступу користувачевого терміналу до мережі і використовується при встановленні з'єднання або реалізації інших процедур, що вимагають виділення індивідуального сигнального каналу;

• MCCH - Multicast Control Channel - однонаправлений канал з конфігурацією точка-багато точок, передає інформацію управління для MBMS від мережі до терміналів користувачів;

• DCCH - Dedicated Control Channel - двонаправлений канал з конфігурацією точка-точка, використовується для передачі індивідуальній сигнальній інформації, якщо між терміналом користувача і мережею існує RRC з'єднання.

Будь-яка передача даних в LTE проводиться по заздалегідь визначеному «графіку передач» в особливих пакетних структурах; у LTE

не існує безперервних «канальних» з'єднань, як в попередніх стільникових технологіях. Складання графіка передач для обох напрямів - завдання MAC-диспетчера в eNodeB, який визначає ресурс, необхідний кожному користувачеві в кожен момент часу. Вирішення про виділення того або іншого ресурсу ґрунтується на отриманих звітах CGI (Channel Quality Indicators) і на інших чинниках.

Розглянемо сукупність каналів, що забезпечують “вертикальну” (між різними рівнями) і “горизонтальну” (між різними вузлами) передачу інформації. На рис. 5.6 показано відображення фізичних, транспортних і логічних каналів в низхідному напрямі.

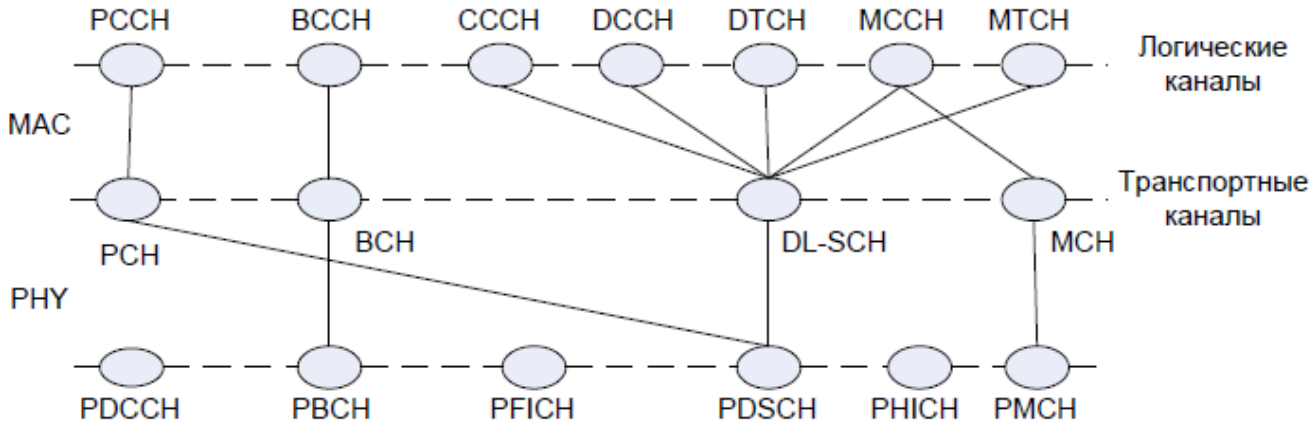


Рис. 5.6 - Відображення фізичних, транспортних і логічних каналів у низхідному напрямі

Передача призначеної для користувача або службової інформації з вищого на нижчий рівень описується в термінах відображення каналів: логічних – на транспортні, транспортних – на фізичні.

Логічний канал PCCH в низхідному напрямі відображується на транспортний викличний канал PCH (Paging Channel), що підтримує переривистий (для економії енергії) прийом пакетів даних.

Логічний канал BCCH відображується або на транспортний мовний канал BCH (Broadcast Channel), або транспортний низхідний спільний канал DL-SCH (Downlink Shared Channel). Канал BCH характеризується фіксованою конфігурацією транспортного блоку, і саме на нього настроюється термінал користувача після синхронізації в соті. У каналі DL-SCH підтримуються адаптивні методи модуляції і кодування, управління потужністю, гібридні автоматичні запити на повторення, багатоантенні технології і ін.

Логічні канали MCCH і MTCH відображуються або в транспортний груповий канал MCH (Multicast Channel), або в транспортний низхідний спільний канал DL-SCH. Канал MCH підтримує групову передачу мультимедійних послуг від декількох сот.

Логічні канали CCCH, DCCH і DTCH відображуються в транспортний канал DL-SCH.

Отже, сім логічних каналів відображуються на чотири транспортні канали. Далі, при переході на фізичний рівень, відбувається відображення транспортних каналів на шість фізичних каналів.

Транспортний канал BCH відображується у фізичний мовний канал PBCH (Physical Broadcast Channel), який передається в часовому інтервалі тривалістю 40 мс., званому кадром.

Транспортні канали PCH і DL-SCH відображуються у фізичний низхідний спільний канал PDSCH (Physical Downlink Shared Channel).

Транспортний канал MCH відображується у фізичний канал групового мовлення PMCH (Physical Multicast Channel).

Три останні фізичні канали: фізичний управляючий канал індикатора формату PCFICH (Physical Control Format Indicator Channel), фізичний управляючий низхідний канал PDCCH (Physical Downlink Control Channel) і фізичний канал індикатора гібридного запиту на повторення PHICH (Physical Hybrid ARQ Indicator Channel) є автономними, тобто на них транспортні канали не відображуються. Канали PDCCH і PCFICH використовується для інформування терміналу користувача про виділення ресурсів для транспортних каналів PCH і DL-SCH, а також параметрів модуляції і кодування. Канал PHICH, як випливає з його назви, використовується для передачі запитів на повторну передачу.

5.2.5 Еволюція мережної архітектури SAE

SAE (System Architecture Evolution) - це мережна архітектура, розроблена з метою безшовної інтеграції мобільної мережі з іншими мережами, що працюють за протоколом IP (рис.5. 7).

У SAE зникають такі елементи, як RNC (Radio Network Controller) і SGSN (Serving GPRS Support Node), а з'являються нові елементи: evolved Node B (eNB), MME (Mobility Management Entity) і SAE Gateway. Це дозволяє мережі отримати «плоску» архітектуру мережі All-IP. SAE здійснює також взаємодію з іншими безпроводовими ні-3GPP мережами (UMTS, WCDMA, WIMAX, WLAN і так далі), дозволяючи мережам з ні-3GPP технологіями мати прямий інтерфейс з мережею LTE і управляти ними в межах однієї мережі LTE/SAE.

SAE включає нове еволюційне пакетне ядро EPC, в яке вбудовані функції взаємодії з іншими безпроводовими мережами. Інтерфейс S2 дозволяє операторам зв'язку розширювати свої мережі іншими заснованими на IP технологіями доступу, управляючи такими функціями, як мобільність, хендовер, білінг, аутентифікація і захист ін- формації в межах мобільної мережі. У EPC використовується також інтерфейс S1 для з'єднання з мережею радіодоступу і інтерфейс S3 для взаємодії з SGSN в цілях підтримки хендовера з мережами GPRS. Інтерфейс SGi призначений для взаємодії EPC і зовнішній IP-мережі.

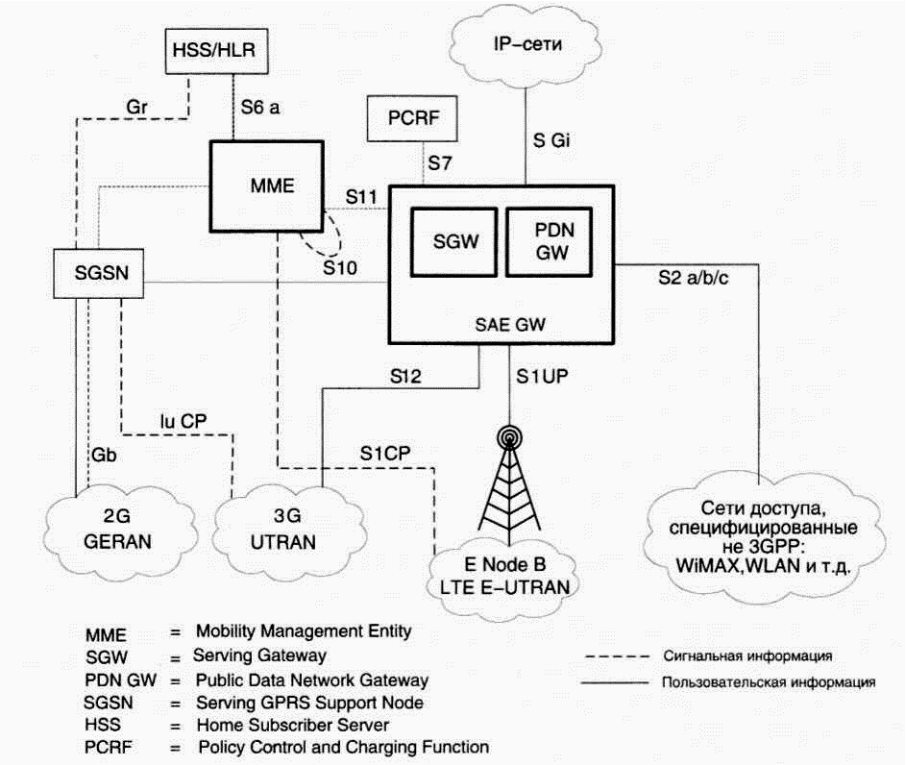


Рис. 5.7 - Еволюція мережної архітектури SAE

Вузол управління мобільністю MME

MME - це центральний елемент опорної мережі LTE, що взаємодіє з обладнанням користувача UE за протоколом NAS.

Функції вузла управління мобільністю охоплюють:

- управління і зберігання даних користувача;
- створення часових ідентифікаторів і їх передачу обладнанню користувача;
- аутентифікацію користувачів;
- управління мобільністю і логічними каналами (bearers).

Процедури управління мобільністю в MME охоплюють пошук і відстежування стану призначеного для користувача пристрою в зоні обслуговування MME, управління установкою і звільненням ресурсів залежно від зміни стані призначеного для користувача терміналу, а також участь в хэндовере.

Аутентифікація і процедури забезпечення захисту мають на увазі взаємодію з базою даних абонентів HSS (Home Subscriber Server), при якому MME здійснює перевірку ідентифікації користувача для захисту від несанкціонованого доступу. Для цього терміналу користувача тимчасово привласнюється спеціальний ідентифікатор, який називається глобальним унікальним тимчасовим ідентифікатором GUTI (Globally Unique Temporary ID), що дозволяє зменшити кількість передач IMSI (міжнародний ідентифікатор мобільного абонента) через радіоінтерфейс. Крім того, MME виконує обмін сигнальною інформацією з SGSN для надання мобільності між 2G/3G і LTE мережами доступу і забезпечує функції

площини управління. Для управління абонентськими профілями і підключення до послуг MME отримує абонентський профіль з HSS домашньої мережі і визначає на базі цього профілю пакетну мережу передачі даних, до якої необхідно підключити пристрій цього абонента.

Обслуговуючий шлюз S-GW

S-GW є шлюзом трафіка користувача, а також трафіка від 3GPP-сетей доступу 2G, 3G і LTE. Підкреслимо, що весь призначений для користувача трафік проходить через S-GW, який є опорною точкою (anchor point) при маршрутизації даних, як в разі пересування користувача в зоні обслуговування LTE, тобто при хендовері між eNodeB, так і в разі забезпечення мобільності між LTE і іншими 3GPP- технологіями доступу. Отже, призначений для користувача трафік маршрутизується через S-GW незалежно від технології радіодоступу, у тому числі в раі зміни її в процесі хендовера. Виникає опорна точка (anchor point), загальна для всіх 3GPP-технологій доступу: 2G/3G/LTE. При цьому, якщо в процесі хендовера змінюється MME, то S-GW також змінюється, але P-GW у всіх випадках залишається незмінним.

Крім того, S-GW відповідає за передачу, маршрутизацію і буферизацію низхідного трафіку даних для UEs, які знаходяться в неактивному стані в мережі LTE, термінує передачу низхідного трафіку для обладнання користувача в стані ECM-IDLE (Idle State Mobility Handling), тобто стає представником користувача, що знаходиться в неактивному стані, а також ініціює запит на обслуговування вхідного сеансу зв'язку, коли трафік потрібно доставити до неактивного обладнання користувача. Для завдань СОРМ (і не лише) підкреслимо, що саме S-GW дублює призначений для користувача трафік в разі його законного перехоплення.

Шлюз пакетної мережі передачі даних P-GW

P-GW (Packet Data Networks Gateway) є граничним маршрутизатором призначеного користувачевого трафіку між EPS і зовнішніми пакетними мережами передачі даних.

У функції P-GW входять розподіл і призначення IP-адресів між обладнанням користувача, забезпечує виконання правил політики і тарифікації PCEF (Policy and Charging Enforcement Function), а саме - управління швидкістю (throttling), управління доступом (gating) і фільтрацію призначених для користувача даних, а також підрахунок використання транспортних ресурсів мережі (трафіку користувача або тривалості сесії). При цьому обладнання користувача може мати декілька одночасних з'єднань через P-GW з багатьма зовнішніми мережами.

Інші мережні елементи LTE

До складу LTE/SAE включаються мережні елементи, використовувані попередніми 3CPP- технологіями. До їх числа входять наступні елементи:

- SGSN (Serving GPRS Support Node) - обслуговуючий вузол підтримки GPRS, призначений для передачі пакетних даних між S-GW і мережею радіодоступу попередніх поколінь 2G і 3G. Для EPS вузол SGSN в перспективі необхідний лише для управління мобільністю між цими системами.

- HSS - сервер абонентів домашньої мережі, призначений для зберігання користувачевих профілів цих абонентів. Також інтегрована в HSS функція забезпечує генерацію даних авторизації і аутентифікації користувача, що зберігаються в HSS. Користувачеві профілі HSS складаються з підписки, інформації безпеки і інформації про місцезнаходження користувача, постійних і тимчасових ідентифікаторів користувача. HSS зберігає дату підключення до послуг, самі послуги, які може отримувати користувач, інформацію про те, до якої зовнішньої мережі пакетної передачі даних підключений користувач. Сервер зберігає також адрес обслуговуючого MME або останнього MME, де був зареєстрований користувач.

- PCRF (Policy and Charging Rules Function) зберігає правила політики по обслуговуванню потоку даних і тарифікації. PCRF забезпечує з боку мережі управління потоками даних залежно від послуг, що надаються, і від QOS, а також управління тарифікацією.

- AAA (Authentication, Authorisation and Accounting) - центр авторизації, аутентифікації і обліку - призначений для обміна інформацією авторизації і аутентифікації з мережами доступу технологій Не-3GPP (Wi-Fi, WIMAX), підключеними до EPC.

5.3 Принципи функціонування радіоінтерфейсу LTE

LTE базується на трьох основних технологіях: мультиплексування за допомогою ортогональних несучих OFDM (Orthogonal Frequency-Division Multiplexing), багатоантенні системи MIMO (Multiple Input Multiple Output) і еволюційна системна архітектура мережі (System Architecture Evolution).

Принципово, що дуплексне розділення каналів може бути як частотним (FDD), так і часовим (TDD). Це дозволяє операторам дуже гнучко використовувати частотний ресурс. Таке рішення відкриває дорогу на ринок тим компаніями, які не володіють спареними частотами. З іншого боку, підтримка FDD дуже зручна для традиційних стільникових операторів, оскільки у них є спарені частоти – таким чином організовані практично всі існуючі системи стільникового зв'язку. Сама ж по собі система FDD істотно ефективніша в плані використання частотного ресурсу, ніж TDD, – в ній менше накладних витрат (службових полів, інтервалів і тому подібне).

Обмін між базовою станцією (БС) і мобільною станцією (МС) будується за принципом кадрів (радіокадрів) тривалістю 10 мс, які циклічно повторюються. Всі часові параметри в специфікації LTE прив'язані до мінімального часового кванта:

$$T_S = \frac{1}{2048 \cdot \Delta f},$$

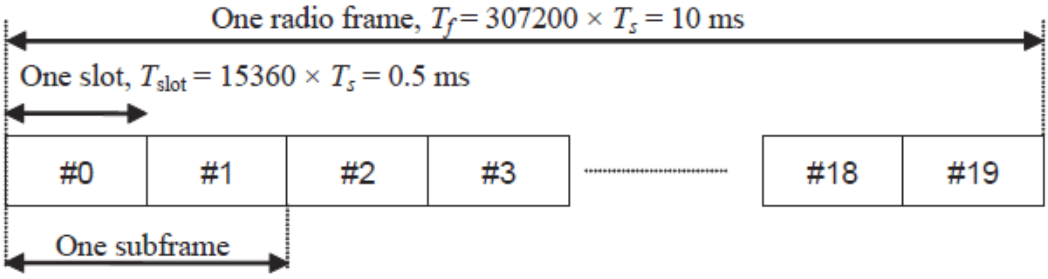
де Δf – крок між піднесучими, що дорівнює 15 кГц (за стандартом).

Таким чином, $T_S = 32{,}5 \cdot 10^{-9}$ $(c.)$, а тривалість радіокадру складає

$$\frac{10^{-3}}{32{,}5 \cdot 10^{-9}} = 307200 T_S$$

Сам же квант часу відповідає тактовій частоті 30,72МГц, що кратно стандартній в 3G-системах (WCDMA із смугою каналу 5 Мгц) частоті обробки 3,84МГц (8×3,84 = 30,72).

Стандарт LTE передбачає двох типів радіокадрів. Тип 1 призначений для частотного дуплексування – як для повного дуплексу, так і для напівдуплекса. Такий кадр складається з 20 слотів (тривалістю 0,5 мс), що нумеруються від 0 до 19. Два суміжні слоти утворюють субкадр (рис.5.8).



Рic.5.8 - Структура кадру LTE при частотному розділенні дуплексних каналів

При повнодуплексному режимі радіокадри у висхідному і низхідному каналах передаються паралельно, але з обумовленим в стандарті часовим зрушенням.

Радіокадр типа 2 (рис. 5.9) призначений лише для часового дуплексування. Він складається з двох напівкадрів тривалістю по 5 мс. Кожен напівкадр включає 5 субкадрів тривалістю 1 мс. Стандарт передбачає два цикли часового дуплексування – 5 і 10 мс. У першому випадку 1-й і 6-й субкадри ідентичні і містять службові поля DWPTS, UPPTS і захисний інтервал GP.

При 10-мс циклі TDD шостий субкадр використовується для передачі даних в низхідному каналі. Нульовий і п'ятий субкадри, а також поле DWPTS завжди відносяться до низхідного каналу, а другий субкадр і поле UPPTS – до висхідного. Можливі декілька варіантів тривалості полів DWPTS, UPPTS і GP, але їх сума завжди дорівнює 1мс.

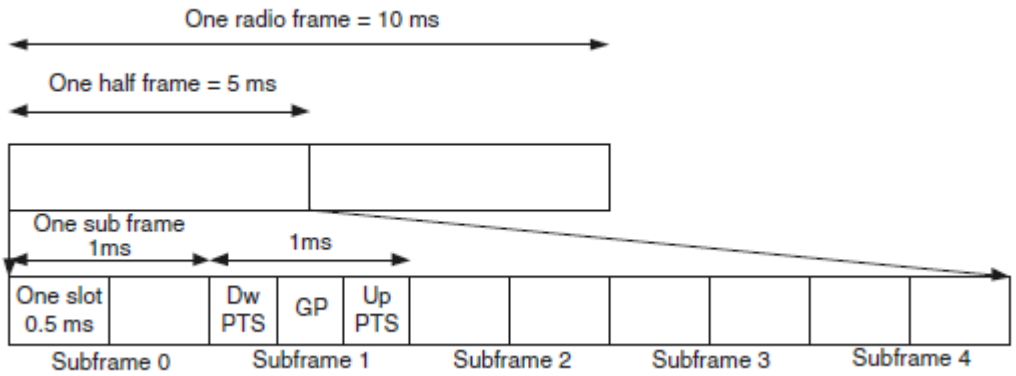


Рис.5.9 – Структура кадру LTE при часовому розділенні дуплексних каналів

У таблиці 5.2 приведені можли ві варіанти конфігурацій “висхідний - низхідний”, формовані для кожного субкадру в межах одного кадру. Символ “D” означає, що такий субкадр зарезервований для низхідного напряму, а символ “U” - для висхідного.

Необхідність переходу від одного напряму до іншого означає наявність в кадрах спеціальних субкадрів, що містять пілотне поле, що зване точкою перемикання, позначається в таблиці 5.2 символом “S”. У цьому полі виділяють спеціальні пілотні слоти низхідного напряму DWPTS (Downlink Pilot Time Slot) і пілотні слоти висхідного напряму UPPTS (Uplink Pilot Time slot), які розташовуються послідовно, разом із захисним полем GP (Guard Period).

Таблиця. 5.2. Варіанти конфігурацій “висхідний - низхідний”

Номер конфігурації	Періодичність точок переключення PTS	Номер підкадрн									
		0	1	2	3	4	5	6	7	8	9
0	5 мс	D	S	U	U	U	D	S	U	U	U
1	5 мс	D	S	U	U	D	D	S	U	U	D
2	5 мс	D	S	U	D	D	D	S	U	D	D
3	10 мс	D	S	U	U	U	D	D	D	D	D
4	10 мс	D	S	U	U	D	D	D	D	D	D
5	10 мс	D	S	U	D	D	D	D	D	D	D
6	5 мс	D	S	U	U	U	D	S	U	U	D

Як видно з приведених даних в таблиці 5.2, можливі конфігурації з періодичністю точок перемикання 5 або 10 мс. При цьому субкадри з періодичністю точок перемикання в 5 мс можливі в обох напівкадрах, тоді як субкадри з періодичністю точок перемикання в 10 мс можливі лише в першому напівкадрі.

У LTE використовується модуляція OFDM, яка передбачає передачу широкосмугового сигналу за допомогою незалежної модуляції вузькосмугових піднесучих вигляду:

$$S_k(t) = a_k \sin(2\pi t(f_0 + k\Delta f)),$$

розташованих з певним кроком по частоті Δf.

Один OFDM-символ містить набір модульованих піднесучих, тобто OFDM-символ є групою несучих частот, яка в даний момент часу переносить біти паралельних цифрових потоків. Завдяки тому, що використовується велике число паралельних потоків, тривалість символу в паралельних потоках виявляється істотно більше, ніж в послідовному потоці даних. У LTE прийнятий стандартний крок між піднесучими Δf = 15 кГц, що відповідає тривалості OFDM- символу 66,7мкс.

У часовій області OFDM-символ включає поле даних (корисна інформація) і так званий циклічний префікс CP (Cyclic Prefix) – повторно передаваний фрагмент кінця попереднього символу (рис. 5.10). Призначення префікса – боротьба з міжсимвольною інтерференцією в приймачі унаслідок багатопроменевого поширення сигналу. Відбитий сигнал, що приходить із затримкою, потрапляє в зону префікса і не накладається на корисний сигнал.

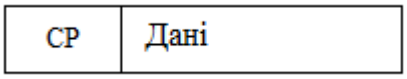


Рисунок 5.10. OFDM - символ з циклічним префіксом

Кожному абонентському пристрою (АП) в кожному слоті призначається певний діапазон канальних ресурсів в частотно-часової області (рис.5.11) – ресурсна сітка. Чарунка ресурсної сітки – так званий ресурсний елемент – відповідає одній піднесучий в частотної області і одному OFDM-символу в часовій.

Ресурсні елементи утворюють ресурсний блок – мінімальну інформаційну одиницю в каналі. Ресурсний блок займає 12 піднесучих (тобто 180 кГц) і 7 або 6 OFDM-символів, залежно від типа циклічного префікса (табл. 5.3) – так, щоб загальна тривалість слота складала 0,5 мс.

Таблиця 5.3 - Фізичний інтерфейс в низхідному каналі при *Δf=15 кГц*.

Тип префіксу	Довжина префіксу		Довжина слоту, OFDM - символів
	T_S	мкс	
Стандартний:			7
перший символ слоту	160	5,2	
останні 6 символів слоту	144	4,7	
Розширений	512	16,7	6

Число ресурсних блоків NRB в ресурсній сітці залежить від ширини смуги каналу і складає від 6 до 110 (ширина частотних смуг висхідного/низхідного каналів в LTE – від 1,4 до 20 Мгц). Ресурсний блок – це мінімальний ресурсний елемент, що виділяється абонентському пристрою планувальником базової станції. Про розподіл ресурсів в кожному слоті базова станція повідомляє в спеціальному управляючому каналі.

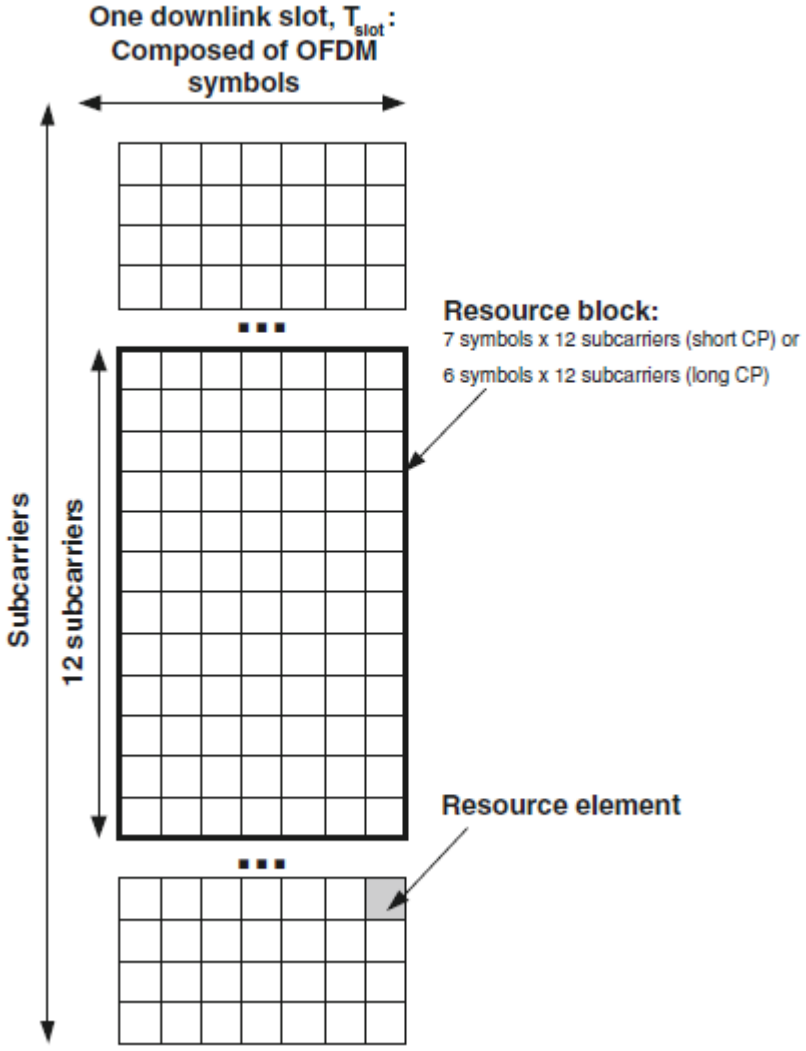


Рис. 5.11 – Ресурсна сітка LTE

Тривалість префікса 4,7 мкс дозволяє боротися із затримкою відбитого сигналу, пройшовшого шлях на 1,4 км. більше, ніж сигнал, що прямо поширюється. Для систем стільникового зв'язку в умовах міста цього зазвичай цілком достатньо. В іншому випадку – використовується розширений префікс, що забезпечує подавлення міжсимвольної інтерференції у чарунках радіусом до 120 км. Такі величезні чарунки корисні для різного роду широкомовних сервісів (MBMS), таких як мобільне ТБ-мовлення. Для цих же режимів (лише у низхідному каналі) передбачена особлива структура слота, з кроком між піднесучими 7,5 кГц і циклічним префіксом 33,4 мкс. У слоті при цьому всього три OFDM-символи. Особливий випадок широкомовного сервісу представляє режим MBSFN (мультимедійний широкомовний сервіс для одночастотної

мережі). У цьому режимі декілька БС в певній MBSFN-зоні одночасно і синхронно транслюють загальний широкомовний сигнал.

Кожна піднесуча модулюється за допомогою 4-, 16- і 64- позиційної квадратурної фазово-амлитудной модуляції (QPSK, 16-QAM або 64-QAM). Відповідно, один символ на одній піднесучий містить 2, 4 або 6 біт. При стандартному префіксі символьна швидкість складе 14000 символів/с, що відповідає, при FDD-дуплексі, агрегатній швидкості від 28 до 84 кбіт/с на піднесучу.

Сигнал із смугою 20 Мгц містить 100 ресурсних блоків або 1200 піднесучих, що дає загальну агрегатну швидкість в каналі від 33,6 до 100,8 Мбіт/с.

Специфікації LTE визначають декілька фіксованих значень для ширини висхідного і низхідного каналу між БС і АС (у мережах E-UTRA). Оскільки в OFDM використовується швидке перетворення Фур'є (ШПФ), число піднесучих для спрощення процедур цифрової обробки сигналу, має бути кратне $N = 2^n$ (тобто 128, 256, ..., 2048). При цьому частота вибірок повинна складати $Fs=\Delta f\ N$. При заданих в стандарті значеннях вона виявляється кратною 3,84 МГц – стандартній частоті вибірок в технології WCDMA. Це дуже зручно для створення багатомодових пристроїв, що підтримують як WCDMA, так і LTE. Зрозуміло, при формуванні сигналу амплітуди "зайвих" піднесучих (включаючи центральну піднесучу каналу) вважаються рівними нулю.

5.4 Технологія OFDM

Фізичний рівень мереж LTE реалізований на базі технології OFDM (мультиплексування з ортогональним частотним розподілом - Orthogonal Frequency Division Multiplexing) і технології SC-FDMA (мультиплексування з частотним розподілом з передачею на одній несучий -Single-Carrier Frequency Division Multiple Access).

Основною метою використання технології OFDM є усунення впливу перешкод, викликаних багатопроменевим поширенням сигналу.

Розглянемо типовий приклад. Хай по радіоканалу проводиться передача інформації з символьною (бодовой) швидкістю 40 МБод за допомогою, наприклад, двійковій фазовій маніпуляції ФМ-2 на тактовому інтервалі $Ts=1/40\cdot10^{-6}$с=25 нс. При цьому сигнали поширюються в замкнутому просторі, який має достатнє число перешкод, викликаючих перевідбиття (вокзал, торгівельний центр і т. п.). У цих умовах прямий і відбиті промені приходять в приймач з відносним запізнюванням, і якщо різниця в затримці стає порівнянною з тривалістю маніпуляційного символу, то починається зростання числа помилок аж до повної втрати інформації, коли, наприклад, два променя приходять в протифазі. Дане явище називається міжсимвольною інтерференцією (MCI).

Так, для даного прикладу при простій схемі багатопроменевого прийому – наявність двох інтерферуючих променів, – запізнювання на один тактовий інтервал виникає, коли різниця ходу прямого і відбитого променів складає

$T_S = 3 \cdot 108$ м/с $\times$ $1/40 \cdot 10^{-6}$ с = 7,5 м,

що типово для більшості сценаріїв мобільного зв'язку.

Проблема міжсимвольної інтерференції могла б бути в значній мірі вирішена, якби тривалість тактового інтервалу, тобто тривалість модуляційного символу, була б істотно (наприклад, на порядок) збільшена. Тоді описана ситуація з виникненням міжсимвольної інтерференції мала б місце на відстанях 102...103 м, що вже не так актуально для реальних сценаріїв. Проте просте збільшення тривалості символів призводить одночасно і до зниження швидкості, що неприйнятно з точки зору забезпечення якості необхідних телекомунікаційних послуг.

Звідси виникає ідея, що полягає в тому, аби розщепнути єдиний високошвидкісний потік, передаваний на одній несучий, на декілька відносно низькошвидкісних потоків, передаючи кожен з них на своїй піднесучий – тобто утворюється конструкція багаточастотних сигналів. Розглянемо цю ідею детальніше.

Отже, використання традиційних одночастотних видів модуляції, коли на одній, чітко вираженій несучий частоті $\omega_0 = 2\pi f_0$ здійснюється передача даних із застосуванням багаторівневих сигналів, є сповна виправданим в умовах, при яких можна нехтувати інтерференційними ефектами, викликаними, головним чином, багатопроменевим поширенням.

Якщо тривалість, відповідна передачі одного елементарного сигналу, рівна T_S, то швидкість передачі інформації R (вимірювана в бітах в секунду) складає:

$$R = \frac{\log_2 M}{T_S},$$

де M - показник, визначальний багатопозиційність використовуваного ансамблю сигналів, тобто кількість можливих станів модульованого сигналу, тоді логарифм цього числа визначає скільки біт даних передається на одному тактовому інтервалі T_S.

Простим способом боротьби з МСІ є збільшення тривалості T_S до тих пір, поки не стане виконуватися умова

$$T_S >> \tau_S,$$

де τ_S - максимальний час затримки поширення при перевідбитті. Тоді можливі спотворення торкнуться лише невеликої частини корисного сигналу, що може виявитися допустимим з точки зору зниження заваадодостійкості. Проте при такому прямому підході виявляються обмеженими можливості по підвищенню швидкості передачі: при фіксованому часі τ_S збільшення значення T_S призводить до зниження R.

Набагато перспективнішим способом боротьби з МСІ, викликаною багатопроменевим поширенням, є відмова від використання сигналів з однією чітко вираженою несучою і використання конструкцій на основі багаточастотних сигналів. Наочною ілюстрацією до побудови таких конструкцій служить концепція розпаралелювання порівняно високошвидкісного потоку даних на сукупність декілька порівняно низькошвидкісних потоків.

Хай B - смуга частот, яку займає дійсний спектр G(f) одночастотного сигналу, і по порядку величини це значення складає $\frac{1}{T_S}$.

Для визначеності покладемо

$$B = \frac{1+\alpha}{T_S},$$

де α – порівнянний з одиницею параметр, значення якого залежить від форми огинаючої елементарного сигналу. Наприклад, для сигналів з прямокутною формою огинаючої і при визначенні ширини спектру по першому нулю α=0. Вибір сигналів з непостійною (що округляє) формою огинає дозволяє забезпечити α<0.

Вважатимемо, що вся смуга частот B розділена на сукупність з K частотних інтервалів (рис. 5.12, де K = 8), які не перетинаються, ширина кожного з них складає B/K, а кожен інтервал відповідає окремому каналу передачі.

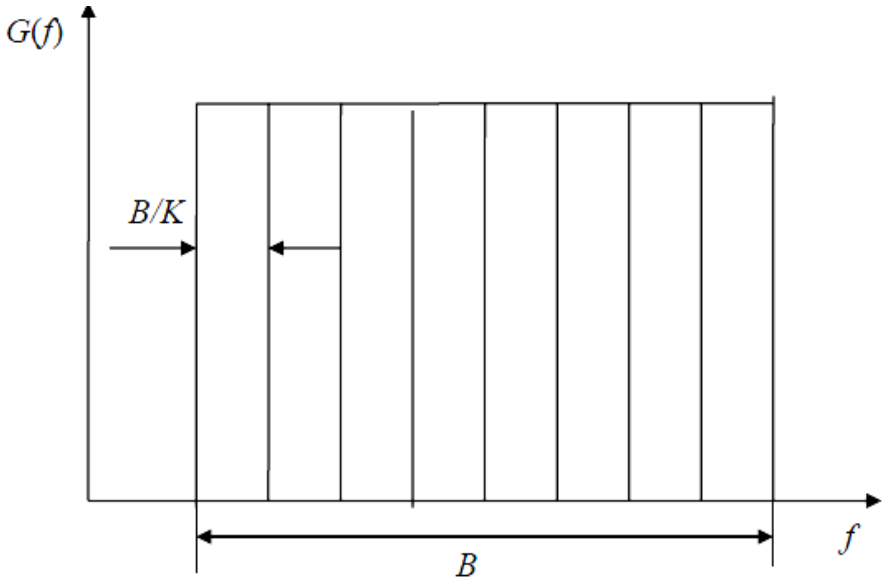


Рисунок 5.12 - Розподіл спектру сигналу на частотні інтервали

Оскільки звуження спектру еквівалентне збільшенню тривалості сигналу в часовій області, можна зробити висновок, що сигнал кожного каналу передачі повинен мати тривалість $K.T_S$, причому спектри таких сигналів будуть локалізовані в частотних інтервалах шириною B/K. При цьому збільшення тривалості відбувається без впливу на обмеження швидкості передачі інформації, оскільки зниження швидкості передачі в окремому каналі компенсується збільшенням числа цих каналів.

Для реалізації і практичного використання описаної концепції потрібно задовольнити ще одній вимозі, що полягає в тому, що окремі канали не повинні перекриватися (як на рис. 5.12), або наявне перекривання якимсь чином повинне компенсуватися - інакше виникнуть міжканальні завади, що призводять до спотворення інформації.

У першому випадку добитися того, аби спектри в різних каналах не перекривалися в принципі можна, ще більш збільшивши тривалість сигналів,

відповідних окремим каналам, добиваючись того, аби рівень спектру спадав до меж інтервалу до заданого значення (рис. 5.13). Проте втрати в швидкості передачі інформації, що виникають при цьому, вже не компенсуватимуться пропорційним збільшенням кількості окремих каналів.

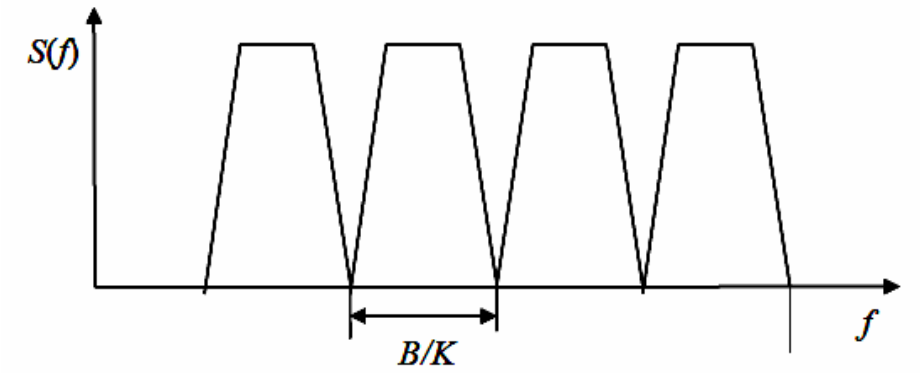


Рисунок 5.13 - Формування спектрів, що не перекриваються

Цій вимозі відповідають ортогональні системи сигналів. В термінах теорії сигналів це означає, що скалярний добуток $(s_k(t), s_l(t))$ між двома будь-якими різними сигналами $s_k(t)$ і $s_l(t)$ з цієї системи дорівнює нулю:

$$\int_0^T s_k(t) \cdot s_k(t) dt = 0,$$

де T - тривалість сигналу.

Спектр будь-якого фінітного сигналу є нескінченим, отже, накладення спектрів буде завжди, проте, саме вживання ортогональних сигналів дозволяє компенсувати перекривання спектрів.

Найпростішою ортогональною системою сигналів $s_1(t), \ldots, s_K(t)$ є набір відрізків гармонійних коливань із заданими значеннями амплітуди A_k, початкової фази φ_k і які відрізняються один від одного певним частотним зсувом:

$$s_k(t) = A_k \cos\left(2\pi f_k t + \varphi_k\right),\ 0 \le t \le T_s.\ k = 0, \ldots, K-1.$$

і якщо сума і різниця частот є цілими кратними значенню $1/T_S$, то скалярний добуток сигналів $(s_k(t), s_l(t)) = 0$. Виберемо $f_k = k/T_S$, тоді отримаємо систему сигналів з ортогональним частотним рознесенням (що відповідає аналітичній формі запису OFDM-сигналу).

$$s_k(t) = A_k \cos\left(2\pi k t / T_s + \varphi_k\right),\ 0 \le t \le T_s.\ k = 0, \ldots, K-1.$$

На рис. 5.14 показаний спектр OFDM- сигналу у вигляді спектральних складових, що отримуються від окремих сигналів.

Видно, що в точках $f_k = k/T_S$ спектр k-го сигналу має максимум, тоді як "хвости" спектрів сусідніх сигналів мають нульові значення. Підкреслимо, що значення частотного інтервалу $\Delta f = 1/T_S$ забезпечує ортогональність сигналів лише для прямокутної форми огинаючої. Вибір сигналів округлої форми огинаючої з таким же значенням частотного інтервалу хоча і дає можливість

отримати компактніший спектр, але спричиняє порушення умови ортогональності і, як наслідок, погіршення завадостійкості.

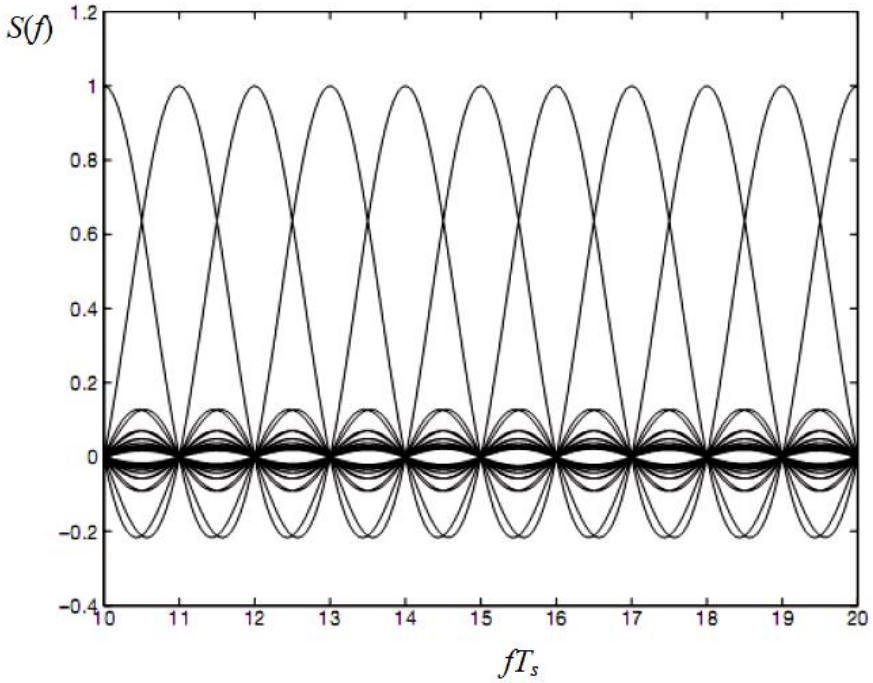


Рис. 5.14 - Спектр послідовності сигналів з ортогональним рознесенням

Звернемося тепер до питання практичної реалізації ансамблю ортогональних багаточастотних сигналів. Прямий спосіб формування, що витікає безпосередньо з опису сигналів, представлений на рис. 5.15.

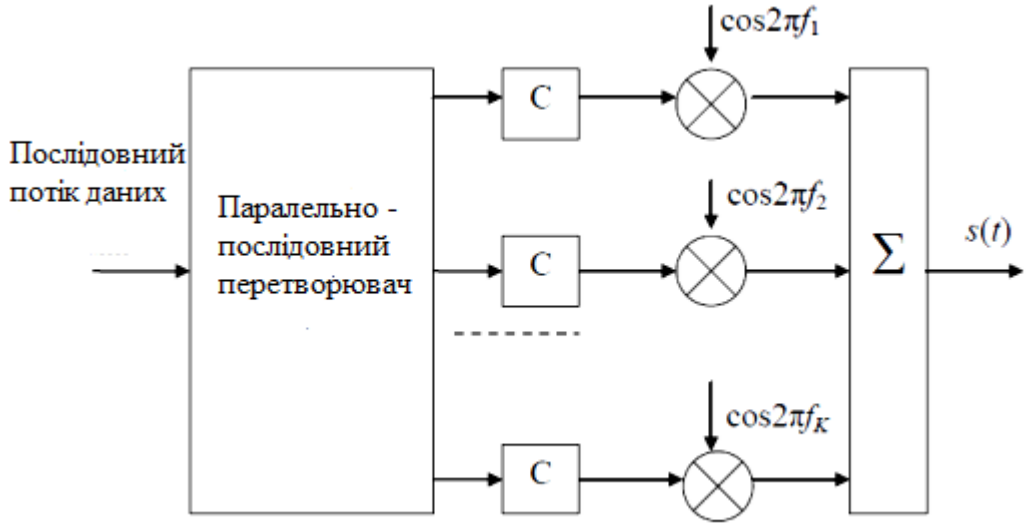


Рис. 5.15 - Структурна схема прямого формування OFDM-сигналів

Формувач складається з перетворювача послідовного потоку даних в паралельний, синтезаторів "С" форми сигналів, що забезпечують заданий вигляд огинаючої, сукупності помножувачів (перетворювачів частоти), що дозволяють перенести спектр сигналів на задані частоти $f_1, \ldots, f_K$, і, нарешті, суматора "Σ", на виході якого і формується багаточастотний сигнал $s(t)$.

При всій очевидності представленого на рис. 5.15 методу формування OFDM-сигналів слід визнати його непрактичність, оскільки він передбачає одночасну роботу *K* синхронізованих за фазою генераторів, що при великих значеннях *K* представляється безперспективним.

Інший підхід, що знайшов своє практичне втілення в сучасних пристроях формування і прийому сигналів, заснований на використанні спеціальної операції цифрової обробки сигналів - дискретного перетворення Фур'є (ДПФ, DFT - Discrete Fourier Transform).

OFDM-сигнал у вигляді суми окремих складових може бути представлений як:

$$s(t) = \sum_{k=0}^{K-1} s_k(t), \quad 0 \le t \le T_S ,$$

Запишемо цей вираз в комплексній формі. Для цього введемо комплексний модуляційний символ $\delta_k = A_k \cdot e^{j\varphi_k}$. Тоді OFDM-символ, побудований на основі сигналів з прямокутною формою огинаючої, можна записати в наступному вигляді:

$$s_{sym}(t) = \mathrm{Re}\left[\sum_{k=0}^{k=K-1} \delta_k \cdot e^{j\frac{2\pi kt}{T_S}} \right] \quad \text{при} \quad 0 \le \mathrm{t} \le \mathrm{T_S}$$

або, вводячи комплексний OFDM-сигнал,

$$\dot{s}_{sym}(t) = \sum_{k=0}^{k=K-1} \delta_k \cdot e^{j\frac{2\pi kt}{T_S}} \quad \text{при} \quad 0 \le \mathrm{t} \le \mathrm{T_S}$$

Таким чином, здійснюючи дискретизацію OFDM-сигналу на інтервалі часу $[0;\mathrm{T_s}]$ з деяким кроком T_0, отримаємо у відлікові моменти часу $t_n = nT_0$ представлення OFDM-символу у вигляді (зворотного) дискретного перетворення Фур'є (ЗДПФ, IDFT - Inverse Discrete Fourier Transform) *K*- елементної послідовності комплексних значень δ_k:

$$\dot{s}_n = \dot{s}_{sym}(t_n) = \sum_{k=0}^{k=K-1} \delta_k \cdot e^{j\frac{2\pi kn T_0}{K \cdot T_0}} = \sum_{k=0}^{k=K-1} \delta_k \cdot e^{j\frac{2\pi kn}{K}} ,$$

яке може бути ефективно обчислене за допомогою всіляких алгоритмів швидкого перетворення Фур'є (ШПФ).

Необхідно врахувати, що алгоритми швидкого перетворення Фур'є передбачають, що число K є двійковою мірою, тоді як реальна кількість піднесучих може виявитися не кратною двом. В цьому випадку обчислення ШПФ проводиться шляхом формального введення в суму нульових доданків, доповнюючих K до двійкової натуральної міри.

Розглянемо вплив міжсимвольної інтерференції (МСІ) на такі сигнали. Основною ідеєю, лежачою в основі боротьби з МСІ, є введення захисного інтервалу, що є частиною тієї тривалості, в межах якої передаються дані. Стосовно даного випадку це означає розділення тривалості T_s OFDM-символу на корисну частину T_u і захисний інтервал Δ. При цьому, з одного боку, в цілях малих втрат в швидкості передачі інформації, бажано, аби T_u істотно перевершував Δ (наприклад, на порядок), а з іншої – захисний інтервал має бути досить протяжним, аби протидіяти МСІ.

На перший погляд реалізація такої ідеї натрапляє на великі складнощі з огляду на те, що наявність захисного інтервалу може привести до спотворення ортогональності елементарних сигналів. Дійсно, якщо спочатку ортогональне частотне рознесення складало $\Delta f = 1/T_s$, то після розділення T_s на T_u і Δ необхідно вибрати $\Delta f=1/T_u$, і, наприклад, на інтервалі [–Δ; T_s-Δ] співвідношення ортогональности перестає виконуватися.

Подолання вказаної проблеми засноване на тому, що частина сигналу, яка передається на тривалості захисного інтервалу, є циклічним префіксом OFDM-символу тобто на інтервалі Δ передається копія частини OFDM-символу, узята “з кінця” корисного інтервалу (на рис. 5.16 заштриховані частини, відповідні циклічному префіксу і тій частині OFDM-символу, з якої цей префікс отриманий).

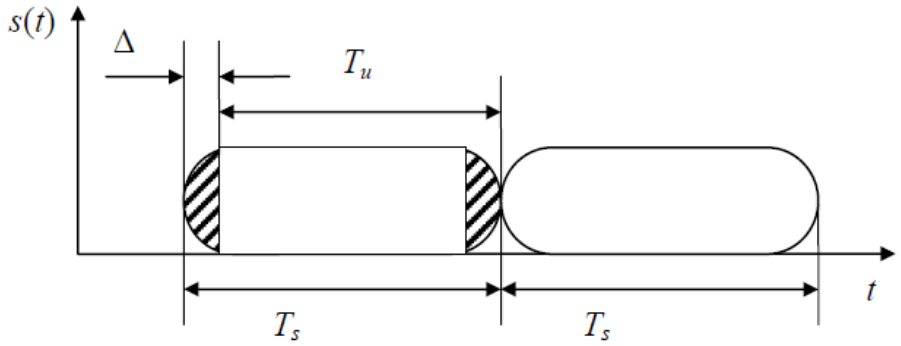


Рис. 5.16 - Формування циклічного префікса

При цьому часове вікно аналізу складає T_u, так що аналізується або безпосередньо корисна частина OFDM-символу (при ідеальній синхронізації), або корисна частина OFDM-символу, відновлена з врахуванням циклічного префікса.

На рис. 5.17 показана структурна схема формування сигналу з OFDM на основі цифрових пристроїв з використанням (програмно або апаратний реалізованого) блоку ЗШПФ.

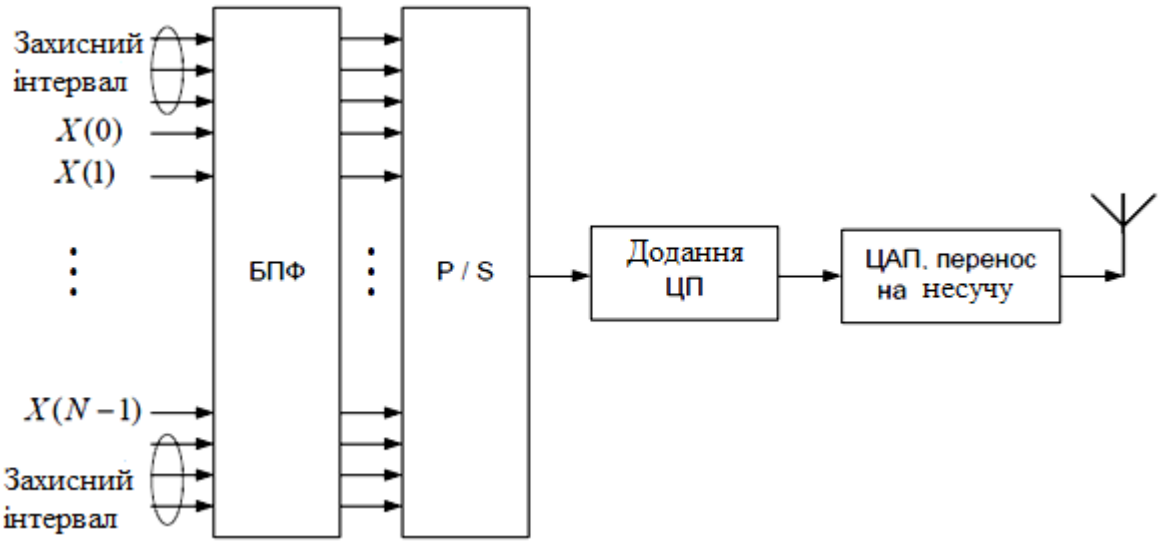


Рисунок 5.17 - Структурна схема прямого формування OFDM-сигналів

N комплексних модуляційних символів δ_k (сигнальні відліки в частотної області), а також G "порожніх" (нульових) символів, призначених для захисних піднесучих, поступають паралельним чином на вхід блоку ЗШПФ, на виході якого утворюються відліки (n = 0, …, N – 1), що є відліками в часовій області. Після цього в межах тривалості інтервалу T_s до них додаються ще відліки, створюючі циклічний префікс. Далі отримані відліки подаються на вхід перетворювача частоти, що реалізує на своєму виході високочастотний радіосигнал. Нарешті, після посилення в блоці посилення потужності такий сигнал подається на вхід антенної системи і випромінюється в ефір.

На практиці частоти несучих відповідають рівнянню

$$s_n(t) = S_0(2\pi f_0 + \frac{n}{T_S})t\,,$$

где f_0 - початок інтервалу, в якому проводиться частотне ущільнення; n - номер несучої, що знаходиться в діапазоні від 0 до (N-1), тобто всього N несучих; T_S - тривалість інтервалу передачі одного.

5.5 Структура сигналів низхідних каналів

У низхідному і висхідному каналі вживання технології OFDM різне. У низхідному каналі ця технологія використовується не лише для передачі сигналу, але і для організації множинного доступу (OFDMA) – тобто для мультиплексування абонентських каналів [5].

Окрім фізичного структурного блоку вводиться поняття логічного структурного блоку. По числу ресурсних елементів вони еквівалентні, проте можливий два варіанти відображення ресурсних елементів фізичного блоку в логічний – один в один і розподілений. У останньому випадку елементи логічного ресурсного блоку виявляються розподіленими по всій доступній

ресурсній сітці. На відміну від пакетних мереж, в LTE немає фізичної преамбули, яка необхідна для синхронізації і оцінки зсуву несучої. Замість цього в кожен ресурсний блок додаються спеціальні пілот- і синхронізуючі сигнали. Пілот-сигнали можуть бути трьох видів – пілот-сигнал, що характеризує чарунку (Cell-specific), сигнал, пов'язаний з конкретним абонентським пристроєм, і сигнал для спеціального широкомовного мультимедійного сервісу. Пілот-сигнал служить для безпосереднього визначення умов в каналі передачі (оскільки приймачу відоме його місцерозташування і вихідна форма). На основі цих вимірів можна визначити реакцію каналу для останніх піднесучих і за допомогою інтерполяції відновити їх вихідну форму.

Пілот-сигнал, що характеризує чарунку, має бути присутнім в кожному субкадрі низхідного каналу. Форма сигналу визначається на основі псевдовипадкової послідовності Голда (варіант m-послідовності), при ініціалізації якої використовується ідентифікаційний номер чарунки БС (Cell ID). Такий пілот-сигнал рівномірно розподілений по ресурсних елементах (рис. 5.18).

Так, при стандартній довжині префікса він транслюється в 0-м і 4-м OFDM-символі, при розширеному CP – під час 0-го і 3-го OFDM-символу. У частотної області опорні сигнали передаються через кожних шість піднесучих, причому зсув визначається ідентифікатором чарунки, взятим по модулю 6.

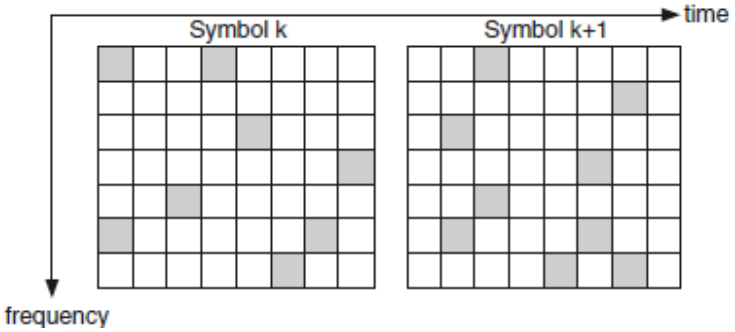


Рисунок 5.18 – Розташування пілот-сигналу LTE

Окрім опорних сигналів, в низхідному каналі транслюються і синхронізуючі сигнали. Синхронізуючі сигнали також однозначно визначають ідентифікаційний номер чарунки БС. У LTE прийнята ієрархічна структура ідентифікації чарунки, як і в попередній їй технології WCDMA. Передбачається, що на фізичному рівні доступно 504 ідентифікаційних номера чарунки БС. Вони розбиті на 168 ID-груп, по 3 ідентифікатори в кожній. Номер групи N1 (0–167) і номер ідентифікатора в ній N2 (0–2) однозначно визначають ID чарунки. Використовується два синхросигнали – первинний і вторинний. Первинний синхросигнал є 62-елементною послідовністю в частотному плані, що задається послідовністю Задова-Чу на основі ідентифікатора N2. Така послідовність з 62 піднесучих, розподілених по ресурсній сітці симетрично відносно її центральної частоти, передається в радіокадрі типа 1 в останньому OFDM-символі слотів 0 і 10 (субкадри 0 і 5). У радіокадрі типа 2 для передачі первинного синхросигналу використовується третій OFDM-символ субкадрів 1 і 6. Вторинний синхросигнал генерується на основі номера ID-групы N1. Він передається в

слотах 0 і 10 радіокадру типа 1 (п'ятий OFDM-символ при стандартному CP) і в слотах 1 і 11 радіокадру типа 2 (шостий OFDM-символ при стандартному CP).

Формування сигналу в низхідному каналі включає процедури канального кодування, скремблювання, формування модуляційних символів, їх розподілу по антенних портах і ресурсних елементах і синтезу OFDM-символів. Канальне кодування передбачає обчислення контрольних сум (CRC-24) для блоків даних, що поступають з MAC-рівня. Потім блоки з контрольними сумами обробляються за допомогою кодера із швидкістю кодування 1/3. У LTE передбачено вживання або згорткового коду, або турбо-коду. Кодована послідовність після перемежування (інтерлівінга) поступає в скремблер (для вхідної послідовності {x(i)} виконується процедура вигляду $dscr(i) = x(i) + c(i)$, де $c(i)$ – визначена скремблююча послідовність). Потім формуються комплексні модуляційні символи (QPSK, 16- і 64-QAM) і розподіляються по ресурсних елементах. Далі відбувається синтез OFDM-символів, їх послідовність поступає в модулятор, що формує вихідний ВЧ-сигнал в заданому частотному діапазоні. На стороні прийому всі процедури виконуються в зворотному порядку.

Рисунок 5.19 – Схема формування сигналу в низхідному каналі LTE

5.6 Структура сигналів висхідних каналів

Застосування OFDM у поєднанні з циклічним префіксом робить зв'язок стійким до часової дисперсії параметрів радіоканалу, в результаті на приймальній стороні стає не потрібним складний еквалайзер. Це дуже корисно для організації низхідного каналу, оскільки спрощується обробка сигналу

приймачем, що знижує вартість термінального пристрою і споживану ним потужність.

У висхідному каналі допустима потужність випромінювання значно нижча, ніж в низхідному. Тому первинною стає енергетична ефективність методу передачі інформації з метою збільшення зони покриття, зниження вартості термінального пристрою і споживаної ним потужності.

Основний недолік технології OFDMA – високе співвідношення пікової і середньої потужності сигналу (PAR). Це пов'язано з тим, що в часової області спектр OFDM-сигналу стає аналогічним Гаусовому шуму, що характеризується високим PAR. Крім того, сама по собі технологія OFDMA, з врахуванням необхідності мінімізувати крок між піднесучими і скорочувати відносну тривалість CP, пред'являє дуже високі вимоги до формування композитного сигналу. Мало того, що частотні розузгодження між передавачем і приймачем і фазовий шум в приймаємому сигналі, можуть привести до міжсимвольної інтерференції на окремих піднесучих (тобто до інтерференції між сигналами різних абонентських каналів). При малому кроці між піднесучими до аналогічних наслідків може привести і ефект Доплера, що дуже актуально для систем стільникового зв'язку, які передбачають високу мобільність абонентів.

В зв'язку з цим для висхідного каналу LTE була запропонована нова технологія – SC-FDMA (Single-Carrier Frequency-Division Multiple Access). Принципова її відмінність – якщо в OFDMA на кожній піднесучий одночасно передається свій модуляційний символ, то в SC-FDMA піднесучі модулюються одночасно і однаково, але модуляційні символи коротші. Тобто в OFDMA символи передаються паралельно, в SC-FDMA – послідовно. Таке рішення забезпечує менше відношення максимального і середнього рівнів потужності в порівнянні з використанням звичайної модуляції OFDM, внаслідок чого підвищується енергоефективність абонентських пристроїв і спрощується їх конструкція (істотно знижуються вимоги до точності частотних параметрів передавачів).

Структура SC-FDMA-сигналу багато в чому аналогічна технології OFDM. Так само використовується композитний сигнал – модуляція множини піднесучих розташованих з кроком Δf. Принципова відмінність в тому, що що всі піднесучі модулюються однаково – тобто одноразово передається лише один модуляційний символ (рис. 5.11).

При цьому ресурсна сітка повністю аналогічна низхідному каналу. Так само кожен фізичний ресурсний блок, відповідний слоту, займають 12 піднесучих з кроком Δf = 15 кГц в частотної області (всього 180 кГц) і 0,5 мс– в часовій. Ресурсному блоку відповідають 7 SC-FDMA-символов при стандартному циклічному префіксі і 6 – при розширеному. Тривалість SC-FDMA-символу (без префікса) дорівнює тривалості OFDMA-символу і складає 66,7мкс (тривалість відповідних циклічних префіксів також рівні). У сітці може бути від 6 до 110 ресурсних блоків, але їх число має бути кратне 2; 3 або 5, що пов'язане з процедурою дискретного Фур'є-перетворення. Ще одна особливість – підтримка модуляції 64-QAM в АП (абоненьському пристрої) є опціональною.

Кожному абонентові мережі для передачі даних від базової станції за допомогою функції планування на певний час виділяється певне число ресурсних блоків. Розклад передається абонентам по службових каналах в низхідному радіоканалі.

Проте якщо при OFDMA один модуляційний символ (QPSK, 16- або 64-QAM) відповідає OFDM-символу на тій, що одній піднесе (15 кГц, 66,7 мкс), то при SC-OFDMA ситуація інша. У частотному плані ширина модуляційного символу виявляється рівною всій доступній смузі частот (він передається на всіх піднесучих одночасно). При цьому один SC-FDMA-символ містить декілька модуляційних символів – в ідеалі стільки ж, скільки піднесучих – але у відповідне число разів коротших в порівнянні з OFDMA, що повністю відповідає умовам теореми Котельникова-Шеннона.

Сама процедура формування SC-FDMA-сигналу відрізняється від схеми OFDMA. Після канального кодування, скремблювання і формування модуляційних символів вони групуються в блоки по M символів – субсимволів SC-FDMA (рис.5.12). Вочевидь, що безпосередньо віднести їх на піднесучі з кроком 15 кГц неможливо – потрібна в N разів вища частота, де N – це число доступних для передачі піднесучих. Тому, сформувавши групи по M модуляційних символів (M < N), їх піддають точковому для M дискретному Фур'є-перетворенню (ДПФ), тобто формують аналоговий сигнал. А вже потім за допомогою стандартної процедури зворотного N-точечного Фур'є-перетворення синтезують сигнал, відповідний незалежній модуляції кожній піднесучий, додають циклічний префікс і генерують вихідний ВЧ-сигнал. В результаті такого підходу передавач і приймач OFDMA- і SC-FDMA-сигналів мають схожу функціональну структуру (рис. 5.10 і 5.12).

Підкреслимо, що АП може використовувати як фіксований частотний діапазон (використовуються суміжні ресурсні блоки, тобто суміжні піднесучі), так і розподілений – так званий режим стрибкоподібної перебудови частоти (FH). У останньому випадку для кожного слоту висхідного каналу використовується новий ресурсний блок з доступної ресурсної сітки. Параметри перебудови частоти задаються мережним устаткуванням і повідомляються як при ініціалізації абонентської станції в мережі, так і по ходу роботи в каналі управління. В разі розподіленого способу – інформація від кожного абонента розташована у всьому спектрі сигналу (рис. 5.13), тому даний спосіб стійкий до частотно-вибіркового завмирання. С іншої сторони, при локалізованому способі розподілу можливо визначити смугу, в якій для даного абонента досягається максимальна стійкість каналу до завмирань. Оскільки області завмирання сигналу для всіх абонентів різні, то можна досягти загальну максимальну ефективність використання радіоканалу. Проте це вимагає безперервного сканування частотної характеристики каналу для кожного пристрою і організації функції диспетчеризації.

Окрім інформації, що генерується функціями верхніх рівнів, у висхідному каналі передаються опорні сигнали. Їх призначення – допомогти приймачу БС налаштуватися на певний передавач АП. Крім того, ці сигнали дозволяють оцінити якість каналу, що використовується в БС при диспетчеризації ресурсів.

Опорні сигнали у висхідному каналі бувають двох видів – так звані "демодульовані" і "зондові" (sounding). Демодульовані опорні сигнали аналогічні опорним сигналам низхідного каналу. Вони передаються на постійній основі. Так, в загальному інформаційному каналі послідовність демодульованого опорного сигналу передається в четвертому SC-FDMA-символі кожного слота при стандартом CP. Зондові сигнали аперіодичні. Їх основне призначення – дати БС можливість оцінити якість каналу, якщо передача ще не ведеться.

5.7 Інформаційні потоки

До цих пір ми говорили про спосіб формування фізичного каналу обміну між абонентськими і базовими станціями. Проте як у висхідному, так і в низхідному каналах передаються різні типи інформаційних потоків.

У висхідному каналі їх три – канал загального користування призначення (PUSCH), управляючий канал (PUCCH) і канал довільного доступу (PURCH). Призначення першого вочевидь – передача інформації користувачів.

Управляючий канал містить таку інформацію, як індикатор якості каналу, повідомлення підтвердження доставки (ACK/NACK) і запит на отримання розкладу (про доступні ресурси). Канал загального користування і управляючий канал ніколи не транслюються одночасно одним АП. Для передачі управляючого каналу використовуються один ресурсний блок в кожному із слотів одного субкадру. Залежно від формату PUCCH можливі чотири варіанти його розташування на ресурсній сітці (рис. 5.14), визначувані змінною ***m***.

Канал довільного доступу служить для запиту початкової ініціалізації в мережі, при хендовері, при переході з режиму чекання в активний режим і тому подібне Абонентській станції призначається інтервал в ресурсній сітці (номер фізичного ресурсного блоку і номер субкадру), протягом якого вона передає спеціальний пакет – преамбулу довільного доступу. Преамбула генерується на основі послідовностей Задова-Чу з нульовою зоною кореляції, всього визначено 64 різних преамбули на одну чарунку. БС, прийнявши запит доступу, відповідає в тому ж самому каналі довільного доступу (але вже низхідному) підтвердженням. Якщо підтвердження не отримане, АП повторює запит.

В низхідному напрямі інформаційних каналів значно більше. Це загальний канал (Physical Downlink Shared Channel - PDSCH); канал управління (Physical Downlink Control Channel – PDCCH); канал групової передачі (Physical Multicast Channel – PMCH); широкомовний канал (Physical Broadcast Channel– PBCH); індикаторний канал управління форматом (Physical Control Format Indicator Channel– PCFICH) і індикаторний канал гібридної процедури повторного запиту (HARQ) Physical Hybrid ARQ Indicator Channel (PHICH). Призначення загального каналу очевидне – передача даних конкретним абонентським пристроям. У каналі управління PDCCH передаються таблиці з призначенням канальних ресурсів абонентським пристроям – як в низхідному, так і у висхідному каналах. У каналі PCFICH, який передається в кожному субкадрі,

вказуються номери OFDM-символів, які використовуються для трансляції повідомлень каналу управління PDCCH. Канал PHICH призначений для підтвердження доставки даних у висхідному каналі. Призначення каналів групової передачі і широкого мовлення також очевидні. Відзначимо особливість широкомовного каналу – кожен блок транспортного широкомовного каналу (з верхніх рівнів протоколу) транслюється в чотирьох субкадрах, наступних з жорстко фіксованим інтервалом в 40 мс. Це виключає необхідність в додаткових покажчиках на розташування цих субкадрів.

5.8 Багатоантенні системи

Як і всі сучасні технології безпроводового зв'язку, в LTE підтримуються багатоантенні системи (MIMO). Враховуючи орієнтацію цієї технології на максимально прості абонентські пристрої, техніка MIMO в LTE максимально спрощена. Стандарт розглядає MIMO-схемИ, 1, 2 і 4 передавальних і приймальних антен в різних поєднаннях. У MIMO-системах є два основні види передачі – просторове мультиплексування і диверсифікована передача. Перший режим означає, що кожен антенний канал транслює незалежний інформаційний потік. При цьому самі канали мають бути некорельованими. Можливі два види просторово-мультиплексованої передачі – для одного АП (SU-MIMO) і для групи АП (MU-MIMO). У першому випадку БС передає декілька незалежних потоків даних одному АП. При цьому в АП повинно бути принаймні не менше антен, чим в БС. У MU-MIMO ресурсні елементи з однаковими частотно-часовими параметрами повинні прийматися до різними АП (при цьому про цифрове формування діаграми спрямованості не йдеться).

Принципово, що одночасно по всіх антенних каналах може передаватися лише два кодові слова (тобто лише два логічно незалежних інформаційних потоки). Тому, не дивлячись на чотири можливі антенні канали, в режимі MU-MIMO БС в одному частотно-часовому діапазоні здатна працювати лише з двома АП.

Диверсифікована передача означає, що декілька антенних каналів використовуються для передачі одного потоку даних. Ця техніка призначена для боротьби із завмираннями в радіоканалі і направлена лише на поліпшення якості передачі в каналі. На швидкість передачі вона впливає опосередковано, через підвищення якості каналу.

У висхідному каналі можлива схема просторового мультиплексування множини абонентів MU-MIMO. Декілька АП, кожний з однією антеною, можуть використовувати однакові частотно-часові ресурси, але за рахунок декорельованих антенних каналів БС працює зі всіма ними одночасно.

5.9 Механізм диспетчеризації і повторні передачі

Під диспетчеризацією розуміється процес розподілу мережних ресурсів між користувачами. Мета диспетчеризації – збалансувати якість зв'язку і

загальну продуктивність системи. У LTE передбачена динамічна і статична диспетчеризація. Динамічна диспетчеризація розподіляє ресурси залежно від поточного стану каналу зв'язку. Вона забезпечує передачу даних на підвищених швидкостях (за рахунок модуляції вищого порядку, зменшення міри кодування каналів, передачі додаткових потоків даних і меншого числа повторних передач), задіюючи для цього часові і частотні ресурси з відносно хорошими умовами зв'язку. Таким чином, для передачі будь-якого конкретного об'єму інформації потрібно менше часу.

Для трафіку сервісів, що пересилають пакети з невеликим корисним навантаженням і через однакові проміжки часу (наприклад, IP-TV), об'єм службової інформації, необхідної для динамічної диспетчеризації, може перевищити об'єм корисних даних. Для таких випадків в LTE передбачена статична диспетчеризація.

Для надійної передачі інформації в технології LTE реалізована система повторної передачі (Hybrid Automatic Repeat Request - HARQ), що стала традиційною. Особливість її реалізації в LTE в тому, що одночасно може підтримуватися декілька (до 8) HARQ-процесів. Якщо дані (субкадр), пов'язані з HARQ-процесом, прийшли успішно, приймач відправляє повідомлення про приймання/неприймання даних (ACK/NACK). В разі відсутності підтвердження або повідомлення NACK відбувається повторна передача. У низхідному каналі розташування і параметри (тип сигнально-кодової конструкції) повторно передаваного субкадру повідомляються додатково, в каналі управління – так звана адаптивна передача, коли БС вибирає оптимальний ресурс для ретрансляції. У висхідному каналі, якщо АП не отримало повідомлення ACK, воно повинне повторити передачу. БС може повідомити АП параметри субкадру для повторної передачі. Якщо ж по каналу управління такого повідомлення не поступило, АП повторює передачу субкадру з точно такими ж параметрами, як і у вихідного субкадру, прийом якого не був підтверджений – неадаптивна ретрансляція. Повторна передача відбувається через задане в специфікації LTE число субкадрів (від 4 до 9), яке залежить від типа дуплексування, типа радіокадру, схеми розподілу каналів в разі TDD і номерів невірно прийнятого субкадру.

5.10 Мережна архітектура SAE

Для технології LTE консорціум 3GPP запропонував нову мережну інфраструктуру (SAE – System Architecture Evolution). Мета і сутність концепції SAE – ефективна підтримка широкого комерційного використання будь-яких послуг на базі IP і забезпечення безперервного обслуговування абонента при його переміщенні між мережами безпровідного доступу, які не обов'язково відповідають стандартам 3GPP (GSM, UMTS, WCDMA і так далі) (рис. 5.15) [5].

В мережі з архітектурою SAE можуть застосовуватися вузли лише двох типів - базові станції (evolved NodeB, eNodeB) і шлюзи доступу (Access Gateway, AGW). Зменшення числа типів вузлів дозволить операторам понизити витрати

як на розгортання мереж LTE/SAE, так і на їх подальшу експлуатацію. Ядро мережі SAE включає чотири ключові компоненти:

- Модуль управління мобільністю (Mobility Management Entity, MME) забезпечує зберігання службової інформації про абонента і управління нею, авторизацію термінальних пристроїв в наземних мережах мобільного зв'язку і загальне управління мобільністю;
- Модуль управління абонентом (User Plane Entity, UPE) відповідає за встановлення низхідного з'єднання, шифрування даних, маршрутизацію і пересилку пакетів;
- 3GPP-якорь грає роль шлюзу між мережами 2G/3G і LTE;
- SAE-якір використовується для підтримки безперервності сервісу при переміщенні абонента між мережами, як відповіднючими специфікаціям 3GPP, так і невідповідаючими (I-WLAN і тому подібне).

Останні два компоненти є абсолютно новими елементами архітектури ядра мережі мобільного зв'язку (Evolved Packet Core) і зобов'язані своєю появою вимозі підтримки мобільності при переміщенні абонента між мережами різних типів.

Функціональні елементи можна по-різному розподіляти серед апаратури мережі. Наприклад, 3GPP-якір допустимо (але не обов'язково) розташовувати разом з модулем управління абонентом. Аналогічно, модулі MME і UPE можна поєднувати або реалізовувати в різних вузлах мережі.

Важлива особливість SAE – призначені для користувача дані можуть пересилатися між базовими станціями безпосередньо, причому як за допомогою проводового, так і безпроводового зв'язку (інтерфейс X2). Це особливо важливо при хендовері, для швидкого безшовного перемикання користувача між БС. Допустимо передавати дані між БС і через шлюзи транспортної IP-сети.

Значна увага в документах 3GPP Release 8 приділена забезпеченню якості сервісу, вибору мережі і використанню ідентифікаційних даних. Поява багатомодових терміналів, призначених, наприклад, для роботи в мережах Wi-Fi і стільниковому зв'язку, дозволяє обслуговувати абонентів із застосуванням різних варіантів доступу. В зв'язку з цим в SAE передбачені механізми вибору найбільш зручної інфраструктури для надання послуг, необхідних абонентові.

Як відзначають розробники SAE, запропоновані ними архітектурні зміни дозволять значно зменшити затримки передачі даних, які особливо критичні для таких застосувань, як VoIP або онлайнові інтерактивні ігри. Зокрема, затримки радіомережі при передачі даних користувача не повинні перевищувати 10 мс (5 мс для коротких IP-пакетів при невеликому мережному навантаженні). Ці значення, принаймні, на 50% краще за аналогічні показники найбільш досконалих мереж 3G.

5.11 Подальші шляхи розвитку LTE

Не чекаючи закінчення робіт над стандартом 3GPP Release8, багато провідних виробників телекомунікаційного устаткування вже представили свої перші дослідні зразки пристроїв, що підтримують LTE. Подальший розвиток

технології LTE продовжуватиметься в рамках робіт над стандартом 3GPP Release 10 (LTE Advanced). На сьогодні вже сформульовані основні вимоги, яким повинен буде задовольняти LTE Advanced. По суті, це вимоги до стандарту мобільних мереж четвертого покоління (4G):

- Максимальна швидкість передачі даних в низхідному радіоканалі до 1 Гбіт/с, у висхідному – до 500М біт/с (середня пропускна спроможність на одного абонента – в три рази вище, ніж в LTE);
- Смуга пропускання в низхідному радіоканалі – 70 МГц, у висхідному – 40 МГц;
- Максимальна ефективність використання спектру в низхідному радіоканалі – 30 біт/с/Гц, у висхідному – 15 біт/с/Гц (втричі вище, ніж в LTE);
- Повна сумісність і взаємодія з LTE і іншими 3GPP системами.

Для вирішення цих завдань передбачається використовувати ширші радіоканали (до 100 Мгц), асиметричне розділення смуг пропускання між висхідним і низхідним каналом в разі частотного дуплексу; досконаліші системи кодування і виправлення помилок; гібридну технологію OFDMA і SC-FDMA для висхідного каналу, а також передові рішення в області антенних систем (MIMO).

Контрольні запитання

1. Назвіть основні особливості мереж безпроводового зв'язку наступного покоління
2. Назвіть основні компоненти фізичної архітектури мережі LTE
3. Назвіть основні компоненти функціональної архітектури мережі LTE
4. Яке призначення шлюзу пакетної мережі P-GW?
5. Яке призначення блоку управління мобільністю MME?
6. Поясните поняття наскрізного каналу (end-to-end bearer).
7. Сформулюйте основне призначення мережної архітектури SAE.
8. Які типи радіокадрів існують в стандарті LTE ?
9. Що таке субкадр ?
10. Запишіть умову ортогональности для двох сигналів.
11. Поясніть, що таке OFDM-символ.
12. Що визначає ресурсна сітка LTE ?
13. Приведіть аналітичний вираз, що визначає залежність швидкості передачі інформації від показника, визначального багатопозицій-ність використовуваного ансамблю сигналів.

Розділ 6. Якість обслуговування (QoS) в мережі NGN

Одним з основних аспектів, який повинен братися до уваги при проектуванні мереж NGN, є забезпечення якості обслуговування. Специфіка пакетних мереж полягає в тому, що, на відміну від мереж з комутацією каналів, в одному і тому ж інформаційному потоці може передаватися різнорідний трафік. При цьому кожен з типів трафіку характеризується рядом критичних і некритичних параметрів.

Для передачі голосового трафіку через пакетні мережі провайдер повинен забезпечити такі умови, які при установці виклику за технологією VoIP гарантують, що флуктуація фази (тобто змінна затримка - variable delay, звана також jitter) відсутня або буде невеликою, затримка передачі даних в одному напрямі не перевищує 150 мс, а гарантована смуга пропускання для потоку даних VoIP знаходиться в інтервалі від 8 до 12 Кбіт/с, за умови, що кодек (CODEC) використовує алгоритм стискування G.729.

Іншими прикладами застосувань, що пред'являють строгі вимоги до смуги пропускання і інших мережних ресурсів, є відеоконференції в реальному часі, передача відеоданих в реальному часі, дистанційне навчання, фінансові транзакції, що вимагають забезпечення безпеки, управління ресурсами, комерційні застосування "Business-to-Business" (B2B) і інші застосування, що вимагають невеликої смуги пропускання, але чутливі до затримки і її змін. Кожне з таких застосувань пред'являє свої вимоги до величини затримки, зміни затримки (джиттеру), до смуги пропускання, імовірності втрати пакетів і доступності служби. Всі перераховані параметри є базовими для технології якості обслуговування. При проектуванні IP-мережі необхідно забезпечити виконання вимог QoS, що пред'являються такими застосуваннями.

Для того, щоб прискорити передачу даних від користувачів або застосувань, багато провайдерів пропонують за додаткову плату служби, визначувані угодами про рівень обслуговування (Service-Level Agreement — SLA). Вживання механізму QoS в IP-мережах надає мережним пристроям можливість вибірково обробляти потоки даних відповідно до угод SLA і забезпечувати виконання мережної стратегії.

Під якістю обслуговування розуміється сукупність механізмів, що дозволяють мережним адміністраторам управляти смугою пропускання, затримкою, варіацією затримки і імовірністю втрати пакетів в мережі.

Механізм QoS не є характеристикою одного пристрою, а є наскрізною системною структурою. Надійне рішення питання про

забезпечення QoS включає розробку ряду взаємодіючих технологій, що дозволяють надавати розширювані і незалежні від середовища служби з можливістю моніторингу роботи всієї мережі. Можливості QoS протоколу IP дозволяють провайдерам задавати пріоритети класам служби, виділяти смугу пропускання і уникати заторів в мережі.

Функції якості обслуговування (QoS) полягають в забезпеченні гарантованого і диференційованого обслуговування мережного трафіку шляхом передачі контролю за використанням ресурсів і завантаженістю мережі її операторові. QoS є набором вимог, що пред'являються до ресурсів мережі при транспортуванні потоку даних. QoS забезпечує наскрізну гарантію передачі даних і заснований на системі правил контроль за засобами підвищення продуктивності IP-мережі, такими як механізм розподілу ресурсів, комутація, маршрутизація, механізми обслуговування черг і механізми відкидання пакетів.

6.1Базові поняття QoS

I. Рівні QoS

Здатність мережі забезпечувати різні рівні обслуговування, що запрошуються тими або іншими мережними застосуваннями, може бути класифікована по таких категоріях:

- *Негарантована доставка даних (best-effort service).* Забезпечення зв'язності вузлів мережі без гарантії часу і самого факту доставки пакету в пункт призначення. Відкидання пакету може статися лише в разі переповнювання буфера вхідної або вихідної черги маршрутизатора. Насправді негарантована доставка пакетів не є частиною QoS унаслідок відсутності гарантії якості обслуговування і гарантії забезпечення доставки пакетів. Негарантована доставка пакетів є на сьогоднішній день єдиною послугою, підтримуваною в Internet. Прикладом, коли ця послуга є достатньою, є взаємодія застосувань по протоколу FTP (File Transfer Protoco).
- *Диференційоване обслуговування (differentiated service).* Диференційоване обслуговування передбачає розподіл трафіку на класи на основі вимог до якості обслуговування. Кожен клас трафіку диференціюється і обробляється мережею відповідно до заданих для цього класу механізмів QoS. Подібна схема забезпечення якості обслуговування (QoS) досить часто називається схемою CoS (Class of Service). Диференційоване обслуговування само по собі не передбачає забезпечення гарантій послуг, що надаються. Відповідно до даної схеми трафік розподіляється по класах, кожен з яких має свій власний пріоритет. З цієї причини диференційоване обслуговування досить

часто називають м'яким QoS (soft QoS). Диференційоване обслуговування зручно застосовувати в мережах з інтенсивним трафіком застосувань.

- *Гарантоване обслуговування (guaranteed service).* Гарантоване обслуговування передбачає попереднє резервування мережних ресурсів по всій траєкторії руху трафіку. Гарантоване обслуговування досить часто називають ще жорстким QoS (hard QoS) у зв'язку з пред'явленням строгих вимог до ресурсів мережі.

II. Характеристики продуктивності мережного з'єднання

Основними характеристиками продуктивності мережного з'єднання є смуга пропускання, затримка, джиттер (тремтіння) і рівень втрати пакетів.

Смуга пропускання (bandwidth) – цей термін використовується для опису номінальної пропускної спроможності середовища передачі інформації, протоколу або з'єднання. Як правило, кожне з'єднання, що потребує гарантованої якості обслуговування, вимагає від мережі резервування мінімальної смуги пропускання (а точніше, пропускній спроможності). Наприклад, застосування, орієнтовані на передачу оцифрованої мови, створюють потік інформації інтенсивністю 64 Кбіт/с. Ефективне використання таких застосувань стає практично неможливим унаслідок зниження пропускної спроможності нижче 64 Кбіт/с на якої-небудь з ділянок з'єднання.

Затримка при передачі пакету (packet delay), або латентність (latency) складається із затримки серіалізації, затримки поширення і затримки комутації.

- Затримка серіалізації (serialization delay) – час, який потрібний пристрою на передачу пакету при заданій ширині смуги пропускання (пропускній спроможності). Затримка серіалізації залежить як від ширини смуги пропускання каналу передачі інформації, так і від розміру передаваного пакету. Наприклад, передача пакету розміром 64 байт при заданій смузі пропускної спроможності 3 Мбіт/с займає всього лише 171 мкс. Затримка серіалізації дуже сильно залежить від смуги пропускання: передача того ж самого пакету розміром 64 байт при заданій смузі пропускання 19,2 Кбіт/с займає вже 26 мс. Досить часто затримку серіалізації називають ще затримкою передачі (transmission delay).

- Затримка поширення (propagation delay). Час, який потрібний переданому біту інформації для досягнення приймаючого пристрою на іншому кінці каналу. Ця величина досить істотна, оскільки в найкращому випадку швидкість передачі інформації порівнянна із швидкістю світла. Затримка поширення залежить від відстані і

використовуваного середовища передачі інформації, а не від смуги пропускання. Для ліній зв'язку глобальних мереж затримка поширення вимірюється в мілісекундах.

- Затримка комутації (switching delay). Час, який потрібний пристрою, що отримав пакет, для початку його передачі наступному пристрою. Як правило, це значення менше 10 нс. Звичайно кожен з пакетів, що належить одному і тому ж потоку трафіку, передається з різним значенням затримки. Затримка при передачі пакетів міняється залежно від стану проміжних мереж.

Якщо мережа не зазнає перевантаження, то пакети не ставляться в чергу в маршрутизаторах, а загальний час затримки при передачі пакету складається з суми затримки серіалізації і затримки поширення на кожному проміжному переході. В цьому випадку можна говорити про мінімально можливу затримку при передачі пакетів через задану мережу. Слід зазначити, що затримка серіалізації стає незначною в порівнянні із затримкою поширення при передачі пакету по каналу з великою пропускною спроможністю. Якщо ж мережа перевантажена, затримки при організації черг в маршрутизаторах починають впливати на загальну затримку при передачі пакетів, і призводять до виникнення різниці в затримці при передачі різних пакетів одного і того ж потоку.

Джиттер-пакетов (packet jitter) – це коливання затримки при передачі пакетів. Даний параметр має велику важливість, оскільки саме він визначає максимальну затримку при прийомі пакетів в кінцевому пункті призначення. Приймаюча сторона, залежно від типа використовуваного застосування, може спробувати компенсувати тремтіння пакетів за рахунок організації приймального буфера для зберігання прийнятих пакетів на час, менший або рівний верхній межі тремтіння. До цієї категорії відносяться застосування, орієнтовані на передачу/прийом безперервних потоків даних, наприклад IP-телефонія або застосування, що забезпечують проведення відеоконференцій.

Втрата пакетів. Рівень втрати пакетів (packet loss) визначає кількість пакетів, що відкидаються мережею під час передачі. Основними причинами втрати пакетів є перевантаження мережі і пошкодження пакетів під час передачі по лінії зв'язку. Найчастіше відкидання відбувається в місцях перевантаження, де число пакетів, що поступають на вхідний інтерфейс мережного вузла, набагато перевищує верхній кордон розміру вихідної черги. Крім того, відкидання пакетів може бути викликане недостатнім розміром вхідного буфера. Як правило, рівень втрати виражається як доля відкинутих пакетів за певний інтервал часу.

Деякі застосування нездатні нормально функціонувати або ж функціонують украй неефективно в разі втрати пакетів. Подібні застосування вимагають від мережі гарантії надійної доставки всіх пакетів.

Як правило, добре спроектовані мережі характеризуються дуже низьким значенням втрати пакетів. Втрата пакетів також невластива застосуванням, для яких були заздалегідь зарезервовані потрібні цим застосуванням ресурси. Що стосується волоконно-оптичних ліній зв'язку із значенням частоти появи помилкових бітів (Bit Error Rate – BER) 10^{-9}, то тут втрата пакетів можлива лише в разі їх відкидання в місцях перевантаження мережі. Відкидання пакетів, на жаль, є неминучим явищем при негарантованій доставці трафіку, хоча і в цьому випадку воно обумовлюється крайньою необхідністю.

Відповідно до Рекомендації MCE-T I.380/Y.1540 основними параметрами, характеризуючими QoS в мережах IP, є:

- затримка перенесення пакетів;
- варіація затримки пакетів (джиттер);
- коефіцієнт втрати пакетів;
- коефіцієнт помилок по пакетах.

Останній параметр залежить в основному від використовуваних на фізичному рівні мережі систем передачі, і проблем з ним, як правило, не виникає. Механізми забезпечення QoS в мережах IP направлені на поліпшення перших три з вказаних параметрів. Саме вони і є основними характеристиками транспортної мережі, що визначають якість передачі мови. Ці ж параметри, як правило, використовуються і в угодах про рівень обслуговування (Service Level Agreement - SLA), запропонованих провідними операторами своїм клієнтам.

III.Функции якості обслуговування

1) Класифікація і маркіровка пакетів

Маршрутизатори, розташовані на кордоні мережі, використовують функцію класифікації для розпізнавання пакетів, що належать різним класам трафіку, залежно від значення одного або декількох полів в заголовку TCP/IP. Функція маркіровки пакетів використовується для розмітки класифікованого трафіку шляхом установки значення поля IP-приоритета або поля коди диференційованого обслуговування (Differentiated Services Code Point – DSCP). Детальніше функції класифікації і маркіровки пакетів розглядаються в наступній лекції.

2) Управління інтенсивністю трафіку

Постачальники послуг використовують обмежуючу функцію для приведення параметрів клієнтського трафіку, що поступає в мережу, відповідно до його профілю. В той же час використовується вирівнююча функція для дозування постачальника послуг трафіку і вирівнювання його інтенсивності, що поступає в мережу, відповідно до заданого профілю.

3) Розподіл ресурсів

Найбільш поширеним механізмом обслуговування черг в маршрутизаторах і комутаторах сучасної Internet є той, що став вже традиційним механізм "першим прийшов, першим вийшов" (first-in, first-out – FIFO). Не дивлячись на простоту реалізації, для механізму FIFO характерні декілька фундаментальних проблем, що утрудняють виконання функцій якості обслуговування. Так, механізм FIFO не передбачає пріоритетної обробки чутливого до затримки трафіку шляхом його переміщення в главу черги. Весь трафік обробляється однаково, без врахування приналежності потоків до різних класів з різними вимогами до обслуговування.

Мінімальна вимога, що пред'являється до алгоритму обслуговування черг, що підтримує функції QoS, – здатність диференціювати і визначати вимоги до обробки різних пакетів. Відповідно до цих параметрів алгоритм обслуговування повинен планувати порядок передачі поставлених в чергу пакетів. Частота обслуговування пакетів одного і того ж потоку трафіку визначає виділену цьому потоку смугу пропускання.

4)Запобігання перевантаженню і політикові відкидання пакетів

Традиційний механізм обслуговування черг FIFO передбачає відкидання всіх вхідних пакетів після досягнення максимального значення довжини черги. Подібний спосіб управління чергою отримав назву "Відкидання хвоста" (tail drop) і характеризується тим, що сигнал про перевантаження поступає лише у момент фактичного переповнювання черги. На жаль, механізм FIFO не передбачає проведення яких-небудь активних дій із запобігання перевантажен

ню або по зменшенню розміру черги з метою зниження часу затримки. Активний алгоритм управління чергами дозволяє маршрутизатору передбачати перевантаження ще до переповнювання черги.

5) Маршрутизація

Традиційна маршрутизація здійснюється на підставі адреса призначення пакету і передбачає вибір найменш короткого маршруту, що зберігається в таблиці маршрутизації. На жаль, подібний механізм є недостатньо гнучким для деяких мережних сценаріїв. Маршрутизація на основі політики – це функція якості обслуговування, що дозволяє замінити традиційний механізм маршрутизації пакетів механізмом, що враховує всілякі параметри, що настроюються користувачем.

Сучасні протоколи маршрутизації, що працюють по методу вибору найменш короткого шляху, дозволяють враховувати такі значення метрики, як адміністративну відстань, вагу або число переходів. Маршрутизація пакетів здійснюється на підставі інформації, що зберігається в таблиці маршрутизації, без врахування вимог потоку трафіку до якості обслуговування або доступності мережних ресурсів на всьому протязі маршруту. QoS-маршрутизація є механізмом маршрутизації пакетів, що враховує вимоги потоків трафіку до якості обслуговування і здійснює вибір маршруту залежно від наявності мережних ресурсів.

Сукупність контрольованих параметрів інформаційного потоку гарантує відповідність між реальними параметрами якості і заданими. Задані параметри визначають допустимі алгоритми його маршрутизації і необхідний об'єм мережних ресурсів. Оператор може використовувати різні механізми управління мережними ресурсами, що забезпечують необхідний рівень QoS. Ці механізми залежать від концепції побудови системи управління мультисервісної мережі і особливостей устаткування, використовуваного у вузлах комутації магістральної мережі.

Механізми забезпечення якості абонентського обслуговування по транспортуванню трафіку в мультисервісній мережі QoS можуть реалізовуватися як на канальному (2-й рівень мережної моделі), так і на мережному (3-й рівень моделі) рівні моделі ISO/OSI:

- механізми QoS канального рівня ATM;
- механізми QoS канального рівня комутованої мережі Ethernet, засновані на класифікації і пріоритезації інформаційних потоків;
- технологія MPLS (MultiProtocol Label Switching), що підвищує ефективність проходження трафіку за рахунок спрощення процесів маршрутизації. Механізм MPLS може бути застосований для забезпечення QoS як в середовищі Ethernet, так і в середовищі ATM.

6.2 Архітектура інтегрованих послуг (IntServ)

6.2.1 Загальні положення

Integrated Service (IntServ, RFC 1633) – модель інтегрованого обслуговування: може забезпечити наскрізну (end-to-end) якість обслуговування, гарантуючи необхідну пропускну спроможність.

В рамках цієї архітектури були розроблені дві послуги – гарантованого обслуговування і регульованого (контрольлваного) навантаження. Гарантоване обслуговування (guaranteed service) передбачає

надання детермінованих гарантій затримки, тоді як служба регульованого навантаження (controlled load service) використовує механізм, схожий на механізм негарантованої доставки трафіку в дещо завантаженій мережі.

Як сигнальний протокол, що використовується для передачі вимог наскрізного обслуговування, IntServ передбачає протокол резервування ресурсів (Resource Reservation Protocol – RSVP).

IntServ можна коротко охарактеризувати як резервування ресурсів (Resource reservation).

Слід зазначити, що модель IntServ вимагає забезпечення гарантованої якості обслуговування для кожного окремого потоку трафіку в масштабах Internet. Враховуючи той факт, що на сьогодні в кожен момент часу в Internet існують тисячі потоків трафіку, об'єм інформації, який повинна підтримувати маршрутизатори, може бути позамежне великим. На жаль, це означає наявність практично неминучих проблем, пов'язаних з масштабуванням мережі, оскільки об'єм інформації, який слід підтримувати маршрутизаторам, збільшується пропорційно зростанню числа потоків трафіку.

6.2.2 Протокол RSVP

Протокол резервування ресурсів (Resource Reservation Protocol – RSVP) є протоколом управління мережею, що дозволяє Internet-застосуванням використовувати різну якість обслуговування (Quality of Service – QoS) для різних потоків даних.

Необхідна швидкість обробки даних мережею залежить від застосування. Деякі застосування, у тому числі традиційні інтерактивні і пакетні, потребують надійної доставки даних, але не пред'являють строгих вимог до її своєчасності. Новіші типи застосувань, такі як відеоконференції, IP-телефонія і інші мультимедійні комунікації, вимагають зворотного: дані повинні доставлятися вчасно, але не обов'язково з гарантією. Протокол RSVP призначений для забезпечення в IP-мережах можливості виконувати різні вимоги по продуктивності, що пред'являються різними типами застосувань.

Важливо відзначити, що RSVP не є протоколом маршрутизації. Він працює спільно з протоколами маршрутизації і створює уздовж маршрутів, що обчислюються за допомогою останніх, еквіваленти списків динамічного доступу. Тому вживання RSVP в існуючій мережі не вимагає переходу на новий протокол маршрутизації.

Протокол RSVP використовується в застосуваннях з груповою розсилкою, таких як застосування аудіо і відеоконференцій. Не дивлячись на те, що спочатку протокол RSVP був орієнтований на мультимедійний

трафік, з його допомогою легко можна резервувати смугу пропускання для однонаправленого трафіку, наприклад для трафіку мережної файлової системи (Network File System – NFS) і трафіку віртуальних приватних мереж, що управляє (Virtual Private Networks – VPN).

6.2.2.1 Потоки даних протоколу RSVP .

В RSVP потік даних є послідовністю дейтаграмм, що мають одне джерело і одержувач (останній може мати як одну, так і декілька фізичних станцій). З поняттям потоку даних тісно пов'язана якість обслуговування. Вимоги QoS передаються по мережі шляхом специфікації потоку (flow specification). Вона є структурою даних, використовуваною вузлами в об'єднаних мережах для запитів спеціальних послуг. Специфікація потоку описує рівень обслуговування потоку даних. Існує три типи потоків даних, відповідних класам обслуговування RSVP.

1. Негарантована доставка (максимальних зусиль - best-effort traffic).
2. Гарантована швидкість (трафік чутливий до швидкості - rate-sensitive traffic).
3. Гарантована затримка (трафік чутливий до затримкі delay-sensitive traffic).

Режимом негарантованої доставки (best-effort traffic) є традиційні потоки даних протоколу IP. Цей режим застосовується при передачі файлів (наприклад, електронної пошти), при електронних транзакціях. Ці застосування вимагають гарантованої доставки даних незалежно від того, скільки часу на це буде потрібно. Для впорядкування прийнятих випадковим чином дейтаграмм і для запиту повторної передачі втрачених і спотворених дейтаграмм передача даних гарантованої доставки спирається на власні механізми протоколу TCP.

Режим гарантованої швидкості (rate-sensitive traffic) вимагає гарантованої швидкості передачі від джерела до одержувача. Прикладом такого застосування є відеоконференції H.323, що працюють під управлінням ISDN (H.320) або ATM (H.310), але застосовувані також в Internet і в багатьох інтранет-мережах протоколу IP.

Режим гарантованої максимальної затримки (delay-sensitive traffic) застосовується до потоків даних, що вимагають своєчасної доставки і відповідної зміни швидкості. Наприклад, швидкість передачі відео MPEG-II коливається від 3 до 7 Мбіт/с, залежно від того, наскільки інтенсивно змінюється зображення. Проте для нормальної роботи кодека необхідно, аби кожен фрейм передавався протягом заданого часу.

6.2.2.2 Обробка потоків даних по протоколу RSVP

На відміну від протоколів маршрутизації, протокол RSVP призначений для управління потоками даних, а не для прийняття рішень відносно кожної дейтаграммы. Потоки даних складаються з дискретних сеансів зв'язку між джерелом і одержувачами. Точніше визначення сеансу – простий потік дейтаграмм до одержувача і протокол транспортного рівня. Таким чином, сеанси ідентифікуються наступними параметрами: адрес одержувача, ідентифікатор протоколу і порт одержувача. Протокол RSVP підтримує як одно-, так і багатоадресні симплексні сеанси.

Примітка. Слід звернути увагу, що сеанси RSVP є симплексними. Таким чином, двонаправлений обмін даними між двома станціями насправді складається з двох окремих симплексних сеансів RSVP.

Для того, щоб запустити багатоадресний сеанс RSVP, одержувач першим приєднується до багатоадресної групи (одержувач вступає в групу розсилки), визначеної IP-адресом одержувача за допомогою протоколу IGMP. При одноадресному сеансі одноадресна маршрутизація виконує ту ж роль, що і IGMP спільно з адресом протоколу PIM (Protocol-Independent Multicast, незалежний від протоколу груповий адрес) для багатоадресного сеансу. Після того, як одержувач приєднається до групи, потенційне джерело починає посилати повідомлення по маршруту RSVP на IP-адрес одержувача. Застосування-одержувач отримує маршрутне повідомлення і починає посилати відповідні запити на резервування, що визначають бажані ознаки потоку, використовуючи протокол RSVP. Після здобуття запиту на резервування застосування-джерело починає відправляти пакети даних.

6.2.2.3 Функціонування протоколу RSVP

Під управлінням RSVP мережні ресурси резервуються для простих (однонаправлених) потоків даних. Логічно кожне джерело відокремлене від одержувача, але будь-яке застосування може бути і джерелом, і одержувачем. Запити на резервування ресурсів виходять від одержувачів.

Кінцеві системи використовують протокол RSVP для запиту в мережі певного рівня QoS від імені потоку даних застосування. RSVP-запити передаються по мережі при проходженні кожного вузла, який застосовується для передачі потоку. Протокол RSVP намагається зарезервувати ресурси для потоку даних на кожному з цих вузлів.

RSVP-сумісні маршрутизатори допомагають доставити потрібні потоки даних в потрібну точку призначення. На рис. 6.1 зображені основні

модулі, інформація про потік даних і інформація про управляючі потоки клієнта і маршрутизатора, що підтримують протокол RSVP.

Перш ніж зарезервувати ресурси, RSVP -демон маршрутизатора з'єднується з двома локальними модулями прийняття рішення – модулем управління доступом (admission control) і модулем управління політикою (policy control). Модуль управління доступом визначає, чи має вузол досить вільних ресурсів для забезпечення запитаного рівня QoS. Модуль управління політикою визначає, чи є у користувача права для того, щоб провести резервування. Якщо яка-небудь з перевірок не пройшла, RSVP -демон відправляє повідомлення про помилку процесу застосування, яке створило запит. Якщо обоє перевірки пройшли нормально, RSVP -демон встановлює параметри класифікатора пакетів (packet classifier) і планувальника пакетів (packet scheduler) для отримання потрібного рівня QoS. Класифікатор пакетів визначає клас QoS для кожного пакету, а планувальник пакетів управляє передачею пакетів, ґрунтуючись на їх класі QoS. Зважений алгоритм рівномірного обслуговування черг (Weighted Fair Queuing – WFQ) і зважений алгоритм довільного раннього виявлення (Weighted Random Early Detection – WRED) забезпечують підтримку QoS на рівні планувальника.

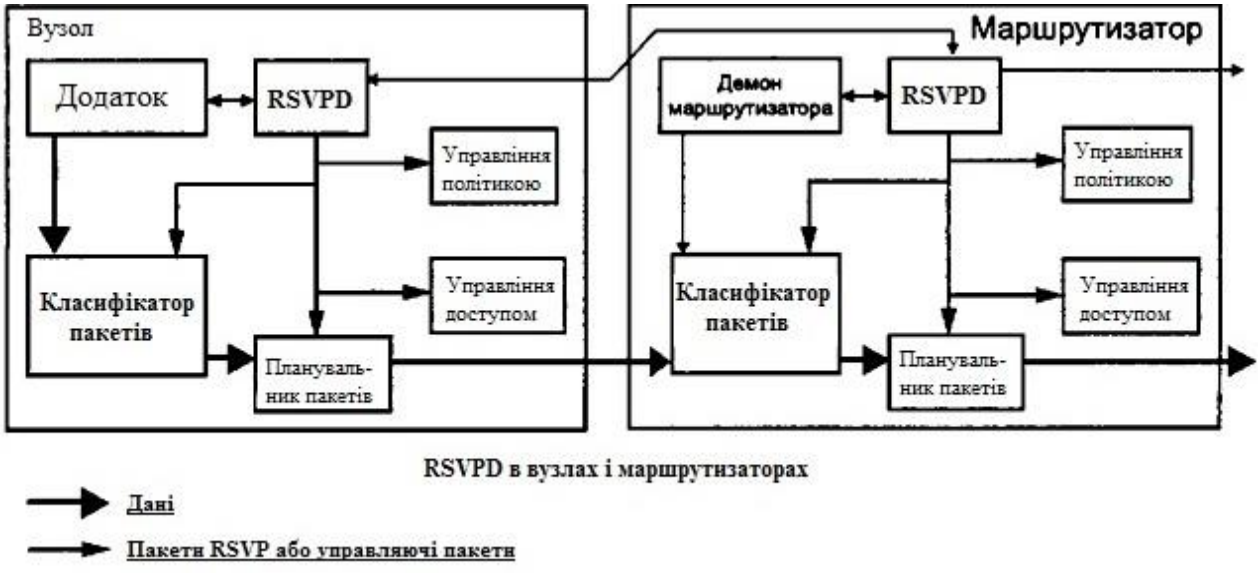


Рис. 6.1-основні модулі RSVP

Під час процесу прийняття рішення модулем управління доступом резервування потрібної смуги пропускання проводиться лише в тому випадку, якщо для запрошуваного класу трафіку досить частини, що залишилася. Інакше запит на доступ відхиляється, але трафік все одно передається з якістю обслуговування, визначеною за умовчанням для даного класу трафіку.

Резервування завжди повинне слідувати по одному і тому же одноадресному щляху або по багатоадресному дереву. В разі виходу з ладу лінії зв'язку маршрутизатор повинен повідомити про це RSVP-демону для того, щоб RSVP-повідомлення, які генеруються їм передавалися по новому шляху.

Алгоритм резервування полягає в наступному. У відповідності з протоколом, відправники інформації розсилають спеціальні повідомлення RSVP Path за унікальною (unicast) або груповою (multicast) адресою. Маршрутизатори, в яких реалізована підтримка протоколу RSVP, отримуючи такі повідомлення, запам'ятовують інформацію про шлях проходження RSVP-трафіку. Одержувачі інформації, що бажають приймати дані з тими або іншими параметрами передачі, відправляють повідомлення RSVP Resv. Це повідомлення пересилається RSVP маршрутизаторами в зворотному, по відношенню до RSVP Path, напрямі. Отримавши таке повідомлення, кожен маршрутизатор, що підтримує RSVP, намагається виконати резервування і пересилає пакет наступному маршрутизатору RSVP на шляху до джерела інформації. Резервування вважається успішним, якщо всім RSVP маршрутизаторам між відправником і одержувачем інформації удалося зарезервувати необхідні ресурси.

Таким чином, IntServ і RSVP наділяють IP-мережу досить потужними можливостями, які дозволяють вельми ефективно передавати дані, чутливі до параметрів передачі. Особливо слід зазначити той факт, що RSVP дозволяє виконувати резервування для кожного окремого мікропотоку (під мікропотоком розуміється сукупність пакетів із зафіксованими значеннями IP-адрес відправника, одержувача і номерами відповідних портів). IntServ є єдиним засобом забезпечення QoS, що підтримує роботу з інформаційними потоками з точністю до мікропотоків.

Алгоритм установки резервування можна розбити на п'ять окремих кроків.

1. Джерела даних посилають управляюче повідомлення RSVP PATH по тому же щляху, по якому вони відправляють звичайний трафік з даними. У цих повідомленнях описуються параметри, що рекомендуються для якісного прийому свого трафіку: верхні і нижні межі пропускної спроможності, затримки і варіації затримки (а також параметри алгоритму корзини маркерів, тобто середня швидкість і глибина корзини; крім того, додатково можуть бути задана максимально допустима швидкість і граничні розміри пакетів потоку). Ці параметри складають специфікацію трафіку джерела.

PATH- повідомлення передається маршрутизаторами мережі у напрямі до всіх вказаних в груповому адресі одержувачів.

2. Кожен RSVP-маршрутизатор перехоплює PATH- повідомлення, зберігає IP-адрес попередньої точки призначення, записує замість нього свій власний адрес і відправляє оновлене повідомлення далі по тому же шляху, по якому передаються дані застосування.
3. Станції-одержувачі після отримання PATH- повідомлення відправляє у зворотному напрямі маршрутизатору, від якого він отримав це повідомлення, запит на резервування ресурсів, тобто RESV- повідомлення. RSVP RESV - повідомлення йдуть від одержувача до відправника в протилежному напрямі по маршруту, пройденому RSVP PATH - повідомлення. На додаток до специфікацій трафіку джерела RESV- повідомлення додатково включає специфікацію запита приймача, в якій вказуються потрібні приймачу параметри якості обслуговування, і специфікацію фільтру, яка визначає, до яких пакетів сеансу застосовувати дане резервування (наприклад, за типом транспортного протоколу і номером порту). Разом специфікації запиту і фільтру є дескриптором потоку, для якого виконується резервування.
4. RSVP - маршрутизатори визначають, чи можуть вони задовольнити ці RESV-запити (чи є в маршрутизатора ресурси, необхідні для підтримки запрошуваного рівня QoS, а по-друге, чи має користувач право на резервування ресурсів). Якщо немає, вони відмовляють в резервуванні. Якщо так, то вони об'єднують отримані запити на резервування і посилають запит попередньому маршрутизатору.
5. Відправники, отримавши запити на резервування ресурсів від відповідних маршрутизаторів, вважають резервування ресурсів таким, що відбулося. Тобто, реальне резервування ресурсів здійснюється RESV- повідомленнями.

Механізм RSVP - резервування схематично показаний на рис. 6.2.

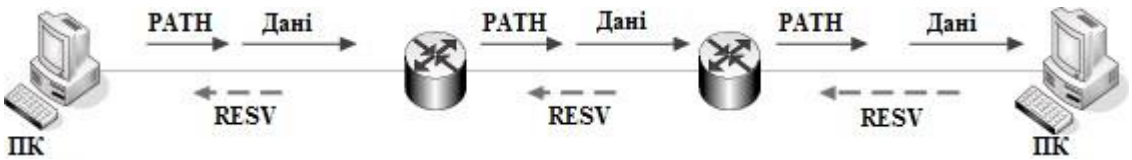


Рис. 6.2 - Механізм RSVP- резервування ресурсів

RSVP-компоненты і функції, які вони виконують:

- RSVP - відправник (RSVP sender) – це застосування, що ініціює відправку трафіку в сеансі RSVP. Нижче перераховані специфікації

потоку, які RSVP - відправники можуть передавати по RSVP - мережі:

- середня швидкість передачі даних;
- максимальний розмір сплеску (Maximum Burst Size – визначається або як максимальний інтервал часу, протягом якого чарунки можуть передаватися відправником з піковою швидкістю PCR, або як максимальна кількість послідовних вічок, які можуть бути передані відправником з тією ж піковою швидкістю PCR).

По мережі, що складається з RSVP - сумісних маршрутизаторів (RSVP-enabled router network), прокладається шлях між RSVP-відправниками і RSVP- одержувачами.

- RSVP-одержувач (RSVP-receiver) – це застосування, яке отримує трафік в сеансі RSVP. Під час конференцій або при передачі голосу по протоколу IP (Voice over IP – VOIP) застосування може грати роль і RSVP-відправника, і RSVP-одержувача. Нижче перераховані специфікації потоку, який RSVP - одержувачі можуть передавати по RSVP - мережі:
  - середня швидкість передачі даних;
  - максимальний розмір сплеску;
  - QoS, включаючи: гарантоване обслуговування – в PATH-сообщениях також описуються максимально можливі затримки в мережі; обслуговування з керованим навантаженням – маршрутизатори гарантують лише те, що мережні затримки будуть мінімальними.

Таблиця 6.1 Повідомлення протоколу резервування ресурсів (RSVP)

Типи повідомлень	Вміст повідомлень
PATH- повідомлення від джерела до приймача	Специфікація трафіка джерела
Специфікація трафіка джерела	Параметри, що рекомендуються, для якісного прийому свого трафіка: верхні і нижні межі пропускної спроможності, затримки і варіації затримки, параметри алгоритму корзини маркерів, тобто середню швидкість і глибину корзини, додатково можуть бути задано максимально допустима швидкість і граничні розміри пакетів потоку
Специфікація фільтру	Визначає, до яких пакетів сеансу застосовувати дане резервування (наприклад, за типом транспортного протоколу і номером порту)

Специфікація запита приймача	Потрібні приймачу параметри якості обслуговування
Дескриптор потоку	Специфікація фільтру плюс специфікація запиту приймача
RESV-повідомлення - запит на резервування ресурсів	Специфікація трафіка джерела плюс дескриптор потоку

6.2.2.4 Стилі резервування

RSVP - резервування ресурсів для потоку можна розбити на два головних типа: індивідуальне і загальне. Простий запит резервування RSVP складається з "flowspec" (специфікація потоку) і "filter spec" (специфікація фільтру); ця комбінація називається "Описувачем потоку". Специфікація flowspec визначає бажане значення QoS.

Filterspec надає інформацію, необхідну класифікаторові пакетів для визначення пакетів, які належать до цього потоку. Flowspec складається із специфікації трафіку (Tspec) і специфікації запиту на обслуговування (RSpec). Tspec описує поведінку трафіку в потоці через маркер параметрів корзини, в той час як RSpec містить вимоги QoS з точки зору пропускної спроможності, затримки, нестабільності передачі і втрати пакетів.

Специфікація фільтру у поєднанні із специфікацією сесії визначають типа набору пакетів.

1) Індивідуальне резервування (FF-Fixed-Filter)

Індивідуальне резервування (distinct reservations) використовується в тих застосуваннях, в яких декілька джерел даних можуть відправляти інформацію одночасно. Стиль FF використовує опції: "чітке" (distinct) резервування і "явний" (explicit) вибір відправника. Таким чином, простий запит за стилем FF створює точно задане резервування для інформаційних пакетів від певного відправника, без спільного використання ресурсу з іншими відправниками в межах однієї і тієї ж сесії. Символічно простий запит резервування FF можна представити як:

FF(S{Q})

де S - вибраний відправник, а Q - відповідна специфікація потоку (flowspec); ця пара параметрів утворюють дескриптор потоку. RSVP дозволяє застосування декількох простих стилів резервування FF одночасно, при цьому формується список дескрипторів потоків:

FF(S1{Q1}, S2{Q2} ...)

У відеозастосуваннях кожен відправник генерує індивідуальний потік даних, для якого необхідно здійснювати окреме управління доступом і планування черги на протязі всього шляху до одержувача. Отже, для такого потоку необхідно здійснювати окреме резервування ресурсів для кожного відправника і для кожного каналу в маршруті.
Найпростіший випадок індивідуального резервування ресурсів спостерігається на прикладі застосування з одноадресним трафіком, де є лише один відправник і один одержувач.

2) Загальне(розділене) резервування (SE-Shared Explicit і WF-Wildcard Filter)

Загальне резервування (shared reservations) використовується в тих застосуваннях, в яких декілька джерел даних не схильні передавати інформацію одночасно, наприклад цифрові аудіозастосування, такі як застосування VoIP. В цьому випадку, оскільки в будь-який окремо взятий проміжок часу розмову веде невелике число людей, інформація передається лише невеликою обмеженою кількістю відправників. Такий потік не потребує окремого резервування ресурсів для кожного відправника, для нього потрібне всього лише одне резервування, яке при необхідності можна буде застосувати до будь-якого відправника в групі.
В термінах протоколу RSVP такий потік називається загальним потоком (shared flow); він встановлюється за допомогою загального явного або групового резервування. Стилі резервування розглядаються нижче.

- При загальному(тому, що розділяється) явному (Shared Explicit – SE) резервуванні потоки, які резервують мережні ресурси, вказуються окремо. Стиль SE використовує опції: резервування, що розділяється (shared), і явний (explicit) вибір відправника. Таким чином, стиль резервування SE формує одне резервування, яке спільно використовується декількома відправниками. На відміну від стилю WF, SE дозволяє одержувачеві безпосередньо специфікувати набір відправників. Запит резервування SE, що містить flowspec Q і список відправників S1, S2 . можна представити в символьній формі як:

  SE((S1,S2...){Q})

  Резервування, що розділяється, виконане із застосуванням стилів WF і SE, придатно для мультикастных застосувань, де декілька джерел даних рідко здійснюють передачу одночасно. Пакетна передача голосу може служити прикладом резервування, що розділяється, оскільки лише обмежене число людей говорять одночасно. Кожен одержувач може направити запит резервування WF або SE на подвоєну смугу пропускання, необхідну одному

відправникові, дозволяючи тим самим говорити обом партнерам одночасно. З іншого боку стиль FF, який здійснює чітке резервування для потоків окремих відправників, підходить для передачі відеосигналів.

- За допомогою групового фільтру (Wildcard Filter – WF) смуга пропускання і характеристики затримки можуть бути зарезервовані для будь-якого відправника (автоматично поширюється на нових відправників при їх появі). Такий фільтр не дозволяє задати відправників окремо – він приймає всіх відправників, на що вказує установка адресу джерела і порту в нуль. Групове резервування WF може розглядатися як загальна труба, чий розмір дорівнює найбільшому з ресурсних запитів від одержувачів і не залежить від числа відправників. Символічно можна представити запит резервування стилю WF як:

  WF(* {Q}),

  де зірочка представляє довільну підстановку при виборі відправника, а Q - специфікація потоку flowspec.

Розглянемо приклади різних стилів резервування. Для простоти представимо flowspec як одновимірне кратне повторення деякої базової якості ресурсу B.

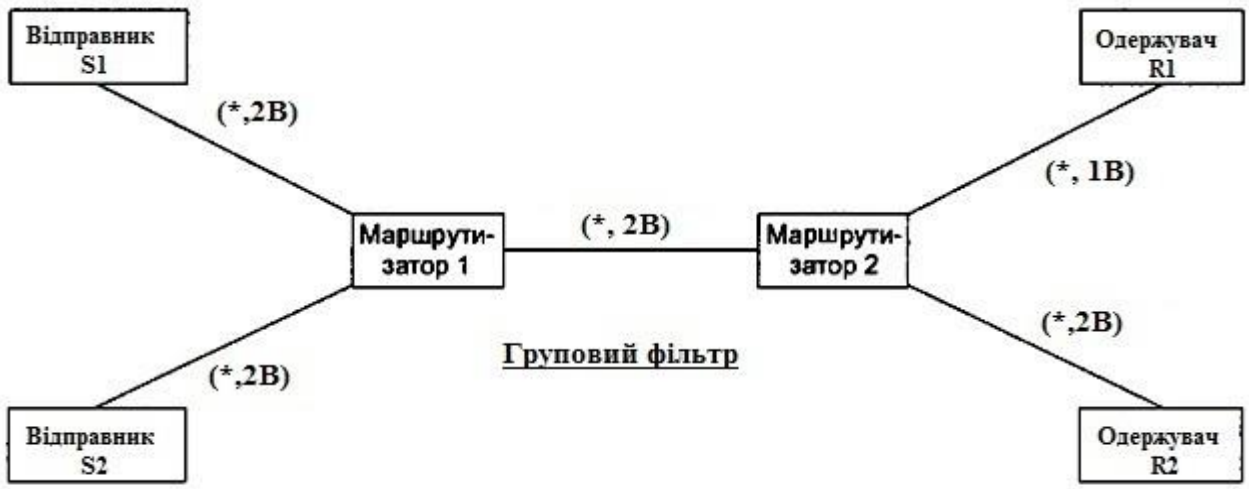
Рис. 6.3 - Приклад резервування FF (Fixed-Filter)

На рис. 6.3 проілюстрований стиль резервування FF (Fixed-Filter). Для кожного одержувача (R1 і R2) є окреме резервування для кожного запитаного джерела, але це резервування буде загальним для всіх одержувачів, які послали запит. Дескриптор потоку для одержувача R2 вкладається в пакет запитів, що направляються вузлу відправникові S2. З іншого боку, два різні дескриптори потоків, що специфікують відправника S1, об'єднуються в один запит FF(S1{2B}), який посилається маршрутизатору 1, а потім вузлу S1.

Для стилю SE результуюча специфікація фільтру є об'єднанням вихідних специфікацій, а результуюча специфікація flowspec рівна найбільшої з flowspec. Обоє джерела отримують ресурс 3В, що розділяється, а запит на виході маршрутизатора 2 можна представити як SE((S1,S2){3B})

Рис. 6.4 - Приклад резервування SE (Shared-Explicit)

При резервуванні враховується той факт, що в точках розгалуження дерева доставки декілька резервованих потоків зливаються в один. Так, в маршрутизаторі 2 в даному прикладі зливаються RESV-повідомлення від приймачів R1 і R2. Якщо для всіх резервованих потоків запрошується однакова пропускна спроможність, то вона потрібна і для загального потоку, а якщо запрошуються різні величини пропускної спроможності, то для загального потоку вибирається максимальна.



Рісунок 6.5 - Приклад резервування WF (Wildcard-Filter)

Рис. 6.5, показує ситуацію, в якій потрібне об'єднання ресурсу для всіх відправників (незалежно від їх кількості) з використанням стилю WF. Кожен з двох вузлів R1 і R2 посилає незалежні запити резервування RSVP, ці два запити

мають бути об'єднані в одну специфікацію flowspec (2B), яка використовується для виконання резервування в маршрутизаторі 1 .

6.2.3 Типи послуг

Протокол RSVP надає два типи інтегрованих послуг, які одержувачі можуть запрошувати за допомогою повідомлень RSVP RESV: службу регульованого навантаження і службу гарантованій бітовій швидкості.

1) Регульоване навантаження

Служба регульованого навантаження (controlled load service) забезпечує гарантію того, що зарезервований потік досягне свого пункту призначення з мінімальним втручанням з боку трафіку, що доставляється без гарантій. Більш того, в реалізації цієї послуги передбачається ізоляція окремих зарезервованих потоків. Ізоляція потоку дозволяє виключити вплив інших присутніх в мережі зарезервованих потоків при резервуванні ресурсів.

Як правило, служба регульованого навантаження застосовується при передачі трафіку Internet-приложений, чутливих до перевантажень в мережі. Такі застосування відмінно працюють в незавантажених мережах, але відразу "приходять в непридатність" при перевантаженні. Прикладом може служити застосування, що працює по протоколу FTP (File Transfer Protocol – протокол передачі файлів).

2) Гарантована бітова швидкість

Служба гарантованій бітовій швидкості (guaranteed bit rate service) забезпечує обмеження затримки без відкидання дейтаграмм, що задовольняють параметрам трафіку, в умовах відсутності збоїв в роботі мережних компонентів або змін в інформації про маршрути під час життя потоку. Ця служба гарантує мінімальне втручання з боку трафіку, що доставляється без гарантій, ізоляцію зарезервованих потоків і числове вираження максимальної затримки.

Служба гарантованій бітовій швидкості може забезпечити лише максимальну, але не мінімальну або середню затримку дейтаграмм.

Максимальна затримка черги – це кумулятивна затримка передачі PATH-повідомлення від джерела до одержувача. PATH- повідомлення містить інформацію про затримку на всій дорозі від джерела до одержувача і у будь-який час надає одержувачеві її точну оцінку. Одержувач використовує інформацію про затримку під час запиту гарантованого обслуговування.

Служба гарантованій бітовій швидкості краще всього личить для тих застосувань масштабу реального часу, які дозволяють відтворювати аудио- і відеофайли.

Служби регульованого навантаження і гарантованої бітової швидкості використовують корзину маркерів для опису параметрів потоку даних. Корзина маркерів – це механізм регулювання інтенсивності трафіку, що визначає середню швидкість (середній об'єм даних, який можна передати за одиницю часу), розмір сплеску (об'єм даних, який можна відправити протягом заданого проміжку часу без збитку для планування черги) і інтервал виміру (квант часу).
При використанні обох служб одержувач запрошує в RESV- повідомленні певну бітову швидкість і розмір сплеску. Планувальник WFQ і механізм управління чергою WRED з переважною вагою гарантують, що трафік досягне одержувача через строго певний час.

Протокол RSVP реалізує резервування, що ініціюється одержувачем. Це можливість, відрізняюча RSVP від інших методів резервування (вживаних, зокрема, в мережах ATM і в мережах ретрансляції кадрів).

Більш традиційним є резервування джерелом ресурсів для даних, які він збирається відправити. Проте такий підхід не годиться для групової розсилки, оскільки у різних членів групи можуть бути різні вимоги в ресурсах. Наприклад, якщо передаваний потік даних може бути роздільний на підпотоки, можливо, деякі члени групи захочуть приймати лише окремі підпотоки, а не весь об'єм передаваної інформації.

Таким чином, у вказаних випадках резервувати ресурси має сенс швидше для одержувачів, чим для відправників. Відправник зобов'язаний надати маршрутизаторам характеристики трафіку, але бажаний рівень обслуговування повинні вказати одержувачі. Маршрутизатори можуть проаналізувати сукупні заявки на ресурси, аби врахувати загальні ділянки в дереві розподілу.

Недоліком протоколу RSVP є те, що об'єм необхідної інформації про стан потоків збільшується із зростанням числа резервувань ресурсів для потоків трафіку.
Оскільки в Internet-магистрали у будь-який час можуть існувати багато сотень тисяч одноадресних і багатоадресних потоків, використання інформації про стан кожного потоку вважається непідходящим рішенням для магістралей Internet.

6.3 Архітектура диференційованих послуг DiffServ

6.3.1 Загальні положення

У 1998 році організація IETF сформувала робочу групу по створенню диференційованих послуг (DiffServ Working Group). Модель *DiffServ*

забезпечує диференціювання трафіку шляхом його розбиття на класи з різним пріоритетом. Відповідно до моделі *DiffServ* забезпечення якості обслуговування в мережі IP передбачає наявність невеликого числа чітко певних “будівельних” блоків, на основі яких можна створити множину різних послуг.

Головним завданням підходу *DiffServ* є визначення стандартизованого байта диференційованої послуги (DS) – байта типа обслуговування (Type of Service – ToS) із заголовка пакету IPv4 і байта класу трафіку (Traffic Class) пакету IPv6. Від даної маркіровки залежить прйняття рішення про просування пакету даних на кожному переході (PHB- per-hop behavior-покрокова поведінка), тобто в кожному проміжному вузлі.

Архітектура диференційованих послуг забезпечує базову основу, яка може бути використана постачальниками послуг для надання своїм клієнтам великого діапазону різних пропозицій залежно від вимог, що пред'являються, до якості обслуговування. Клієнт може вибрати необхідний рівень послуг шляхом установки відповідного значення поля коди диференційованої послуги (Differentiated Services Code Point – DSCP) для пакетів певного застосування. Код диференційованої послуги визначає ланцюжок рішень про просування пакету в кожному проміжному вузлі мережі постачальника послуг (PHB- олітика).

На рис.6.6 зображено узагальнену операційну модель QoS.

Рис 6.6 - Узагальнена операційна модель QoS

Формування трафіку включає виконання таких функцій, як:

- класифікація пакетів (установка значення поля DSCP);
- обмеження трафіку.

Формування трафіку зазвичай здійснюється на вхідному інтерфейсі *DiffServ*-домена, на який поступають пакети. Формування грає вирішальну роль в управлінні трафіком, який поступає в *DiffServ*-домен, оскільки в цьому випадку для кожного пакету мережа може визначити відповідну йому PHB-політику.

На рис. 6.7 схематично представлена архітектура диференційованих послуг. Опис двох основних функціональних блоків цієї архітектури приведений в таблиці.

Таблиця 6.2 Функціональні блоки архітектури диференційованих послуг

Функціональний блок	**Розташування**	**Функція**	**Дія**
Формувачі трафіку	Вхідний інтерфейс граничного маршрутизатора *DiffServ* -домена	Класифікація пакетів, вирівнювання і обмеження трафіку	Обмеження вхідного трафіку і установка значення поля DSCP на основі профілю трафіку
Пристрої, що реалізовують PHB-політику	Всі маршрутизатори *DiffServ* -домена	Розподіл ресурсів і політика відкидання пакетів	PHB-політика обробки пакетів визначається на основі характеристик якості обслуговування відповідних заданому значенню поля DSCP

PHB-політика – політика покрокового обслуговування, визначає поведінку мережного вузла відносно пакетів з певним значенням поля коду диференційованої послуги (DSCP). Всі пакети потоку трафіку із специфічною вимогою до обслуговування несуть в собі одне і те ж значення поля DSCP. Всі вузли усередині *DiffServ* -домена визначають PHB-політику, яка має бути застосована до пакету на основі значення поля коду диференційованої послуги, що зберігається в нім. Крім того, граничні вузли *DiffServ*-домена виконують важливу функцію формування трафіку, що поступає в *DiffServ* -домен.

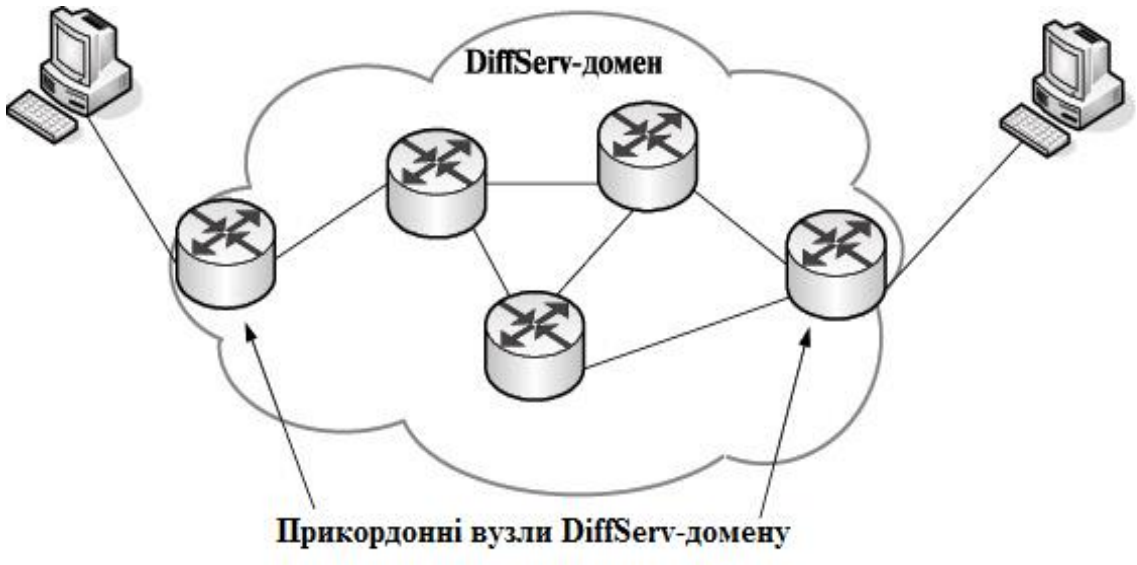


Рис. 6.7 - Архітектура методу DiffServ

6.3.2 Код диференційованої послуги (DSCP - Differentiated Services Code Point)

Диференціальний вид послуг зазвичай передбачає використання 6-бітового поля DSCP (DiffServ Code Point). Запис в полі DSCP зазвичай здійснюється на вході мережі. Поле DS (Differentiated Services), де розміщується DSCP, фактично заміщає поле ToS (RFC-791) в IP-заголовку.

Фактично код диференційованої послуги є розширенням 3-бітового поля IP-пріоритету. Так само, як і IP-пріоритет, код диференційованої послуги дозволяє визначати спосіб обробки відмічених відповідним чином пакетів даних. На рис. 6.8 представлена структура байта ToS. Після стандартизації поля коди диференційованої послуги байт ToS буде перейменований в байт DS. На рис. 6.9 представлена структура байта DS.

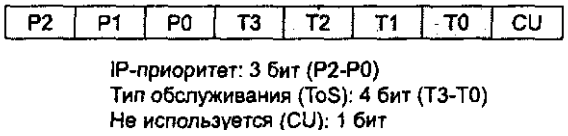


Рис. 6.8 - Структура байта ToS у відповідності з RFC 1349

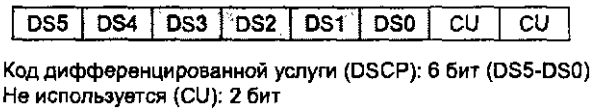


Рис. 6.9 -- Структура байта DS

На сьогоднішній день робоча група IETF по створенню і впровадженню диференційованих послуг визначає коди DSCP таким чином:

- Стандартний код DCSP визначений як 000 000.
- Селектор класу. Ці коди DCSP мають зворотну сумісність з кодами IP-пріоритету і представлені нижче.

Селектор класу	DSCP
Пріоритет 1	001 000
Пріоритет 2	010 000
Пріоритет 3	011 000
Пріоритет 4	100 000
Пріоритет 5	101 000
Пріоритет 6	110 000
Пріоритет 7	111 000

- PHB- політика негайної передачі (Expedited Forwarding — EF). Цей код DSCP відповідає найбільш висококласному рівню обслуговування, що надається за додаткову вартість. Значення, що рекомендується, — 101 110.

• PHB - політика гарантованої передачі (Assured Forwarding — AF). Ці коди DSCP визначають чотири рівні обслуговування, кожен з яких, у свою чергу, може бути охарактеризований трьома рівнями пріоритету відкидання даних.

PHB-політиці гарантованої передачі відповідають 12 кодів DSCP, представлених в таблиці 6.3.

Таблиця 6.3 Коди DSCP для потоків з політикою гарантованої передачі

Пріоритет відкидання пакету	Клас 1	Клас 2	Клас 3	Клас 4
Низький	AF11 001010	AF21 010010	AF31 011010	AF41 100010
Середній	AF12 001100	AF22 010100	AF32 011100	AF42 100100
Високий	AF13 001110	AF23 010110	AF33 011110	AF43 100110

6.3.3 Формування трафіку на границі мережі

Функції формування трафіку, реалізовані в граничних пристроях мережі. До цих функцій відносяться функції класифікації трафіку, маркіровки пакетів і управління інтенсивністю трафіку. Граничні функції класифікують або маркірують трафік шляхом установки відповідного значення поля DSCP, а також проводять моніторинг вхідного в мережу трафіку з метою перевірки його відповідності встановленому профілю.

Traffic profile - профіль трафіку - опис часових характеристик потоку трафіку (таких, як швидкість і пікова швидкість).

Розглянемо детальніше механізми, що реалізовують ці функції.

6.3.3.1 Класифікація пакетів

Класифікація пакетів (packet classification) є засобом, що дозволяє віднести пакет до того або іншого класу трафіку залежно від значення одного або декількох полів пакету. Функція, що розпізнає, може бути як дуже простою, так і вельми складною. Нижче перераховано декілька різних способів класифікації пакетів.

- Функція, що розпізнає IP-поток, залежить від п'яти параметрів: адрес джерела IP-пакета, адрес призначення IP-пакета, поле протоколу IP, порт джерела і порт призначення. Потік інформації складається з пакетів, які

згенеровано застосуванням, яке виконується на комп'ютері-джерелі, і які призначаються для передачі застосуванню, яке виконується на комп'ютері-приймачі. Пакети, що належать одному потоку, мають однакові значення всіх п'яти полів в заголовку IP-пакета. Таким чином, розпізнавальна функція ідентифікує потік.

- Розпізнавальна функція залежить від значення поля IP-пріоритету або поля коду диференційованої послуги (DSCP). Це найбільш поширений спосіб класифікації пакетів
- Розпізнавальна функція залежить від інших параметрів заголовка TCP/IP- пакету, таких, як довжина пакету.
- Розпізнавальна функція залежить від MAC-адреса джерела і MAC-адреса призначення пакету.
- Розпізнавальна функція залежить від використовуваних застосуванням номерів портів, адреса URL (Universal Resource Locator – універсальний покажчик інформаційного ресурсу) і так далі. Розпізнавання застосувань на основі мережних параметрів (NBAR) дозволяє маршрутизаторам ідентифікувати трафік окремих застосувань, дозволяючи таким чином проводити класифікацію пакетів на основі програмних засобів, що їх згенерували.
- Розпізнавальна функція визначається на підставі значення поля QoS-групи, що відноситься до внутрішньої по відношенню до маршрутизатора структури даних пакету.
- Розпізнавальна функція визначається на підставі вхідного інтерфейсу маршрутизатора.

Всі пакети, що належать певному класу трафіку “забарвлюються” у відповідний колір, тобто маркіруються.

6.3.3.2 Маркіровка пакетів

Функція маркіровки використовується для ідентифікації відповідного класу трафіку або, часто говорять, для “розфарбовування” класифікованого трафіку шляхом установки відповідного значення поля IP-пріоритету або поля коду диференційованої послуги (Differentiated Services Code Point – DSCP), розташованих в заголовку IP-пакета, а також шляхом установки значення поля QoS-групи, що відноситься до внутрішньої по відношенню до маршрутизатора структури даних пакету. Попавши в ядро мережі, “розфарбовані” пакети будуть оброблені відповідно до PHB-політики, визначеної на підставі поля IP-приоритета, або поля DSCP або QoS-группы. Таким чином, ця функція призначена для

запису/перезапису поля DSCP залежно від класу трафіку, до якого відноситься даний пакет.

1) IP-пріоритет

Поле IP-пріоритету, розташоване в заголовку IP-пакета, вказує на відносний пріоритет при обробці відповідного пакету даних. Поле IP - пріоритету складається з трьох бітів байта типа обслуговування (Type of Service – ToS). Окрім бітів IP-пріоритету, байт ToS містить біти типа обслуговування (ToS-біти). ToS-біти були призначені для зберігання значень, що визначають спосіб обробки відповідного пакету даних в мережі, проте на практиці вони не набули широкого поширення. Схема байта ToS, що включає біти IP-пріоритету і ToS-біти була розглянута вище. У таблиці перераховані всі допустимі комбінації бітів IP-пріоритету разом з їх значеннями і назвами.

Таблиця 6.4 Значення IP-пріоритету

Значення IP-пріоритету в десятковій формі вистави	Значення IP-пріоритету двійковій формі вистави	Назва IP-пріоритету
0	000	Стандартний
1	001	Пріоритетний
2	010	Негайний
3	011	Терміновий
4	100	Надстроковий
5	101	Критичний
6	110	Міжмережне управління
7	111	Мережне управління

Примітка. *За умовчанням всьому управляючому трафіку, відповідальному за забезпечення маршрутизації, ставиться у відповідність IP-пріоритет 6. Окрім цього, для трафіку управляючої мережі зарезервований також і IP-пріоритет 7. Отже, IP-пріоритет 6 і 7 не рекомендується призначати трафіку призначених для користувача застосувань***.**

“Розфарбовування” пакетів шляхом установки значення поля IP-пріоритету може бути здійснене як застосуванням, що згенерувало ці пакети, так і вузлом мережі.

Примітка. *Засоби якості обслуговування Cisco, що підтримують функцію маркіровки пакетів, включають механізм узгодження швидкості доступу (Committed Access Rate – CAR), маршрутизацію на основі політики (Policy-Based Routing - PBR) і поширення політик QoS за допомогою протоколу граничного шлюзу (QoS Policy Propagation using Border Gateway Protocol - QPPB).*

2) DSCP

Поле DSCP складається з шести бітів заголовка IP. Схема байта DSCP розглядалася вище. Аналогічно IP-пріоритету, поле DSCP є частиною заголовка IP-пакета. Насправді поле DSCP є розширенням поля

IP-пріоритету. Отже, способи використання і установки значення поля DSCP багато в чому нагадують розглянуті нами раніше способи використання і установки значення поля IP-пріоритету. Слід зазначити, що поле коду диференційованої послуги (DSCP) має зворотну сумісність з полем IP-пріоритету.

3) QoS-група

QoS-група є полем внутрішньої по відношенню до маршрутизатора структури даних пакету. Поле QoS-групи застосовується для маркіровки пакетів на підставі визначених користувачем критеріїв класифікації. Слід зазначити, що поле QoS-групи є внутрішнім по відношенню до маршрутизатора і не входить в заголовок IP-пакету.

Модульний інтерфейс командної строки QoS дозволяє проводити маркіровку пакетів з використанням будь-якого з трьох розглянутих вище механізмів. У таблиці 6.5 приведена порівняльна характеристика механізмів маркіровки пакетів за допомогою поля IP-пріоритету, поля DSCP і поля QoS-групи.

Таблиця 6.5 Маркіровка трафіку з використанням поля IP-пріоритету, поля DSCP і поля QoS-групи

Атрибути	IP-пріоритет	DSCP	QoS-група
Область класифікації	Вся мережа. Значення поля IP-пріоритету зберігається в заголовку IP-пакету	Вся мережа. Значення поля DSCP зберігається в заголовку IP-пакету	Внутрішнє поле по відношенню до заданого маршрутизатора. Значення поля QoS - групи не зберігається в заголовку IP-пакету
Кількість класів	8 класів (0-7)	64 класу (0-63)	100 класів (0-99)

Досить часто пакети поступають в граничний пристрій мережі з вже встановленим полем IP-пріоритету або полем DSCP. Не дивлячись на те що пакет, що поступив, вже має “розфарбовування”, мережний оператор повинен призначити нову маркіровку пакету залежно від його класу і відповідного цьому класу якості послуг, пропонованих даною мережею

Приклад. Класифікація і маркіровка пакетів з використанням поля IP-пріоритету.

Постачальник послуг Internet (Internet Service Provider – ISP) пропонує різні рівні обслуговування трафіку клієнта з використанням для цих цілей поля IP- пріоритету (іншими словами, він гарантує переважну

обробку клієнтського трафіку в межах своєї базової мережі). Корпоративний клієнт оплачує ISP два рівні послуг.

Трафік корпоративного клієнта, що поступає в мережу ISP з мережі 215.215.215.0/24, повинен мати значення поля IP-пріоритету, що дорівнює 5, а весь трафік, що залишився, – значення поля IP-пріоритету, що дорівнює 4 (рис. 6.10).

З метою установки значення поля IP-пріоритету всього вхідного трафіку на підставі IP-адреса джерела постачальник послуг Internet повинен застосувати відповідні конфігураційні команди механізмів узгодження швидкості доступу (CAR), маршрутизації на основі політики (PBR) або поширення політик QoS за допомогою протоколу граничного шлюзу (QPPB) на високошвидкісному послідовному інтерфейсі маршрутизатора (High-Speed Serial Interface – HSSI), підключеного до мережі корпоративного клієнта. Наприклад, можна використовувати відповідні команди (оператори) управління конфігурацією маршрутизатора, що привласнюють певній групі доступу на вказаному інтерфейсі HSSI, пріоритет 5 трафіку, що поступає з мережі 215.215.215.0/24. Всьому трафіку, що залишився, і який поступає на інтерфейс HSSI, привласнюється значення поля IP- пріоритету, рівне 4.

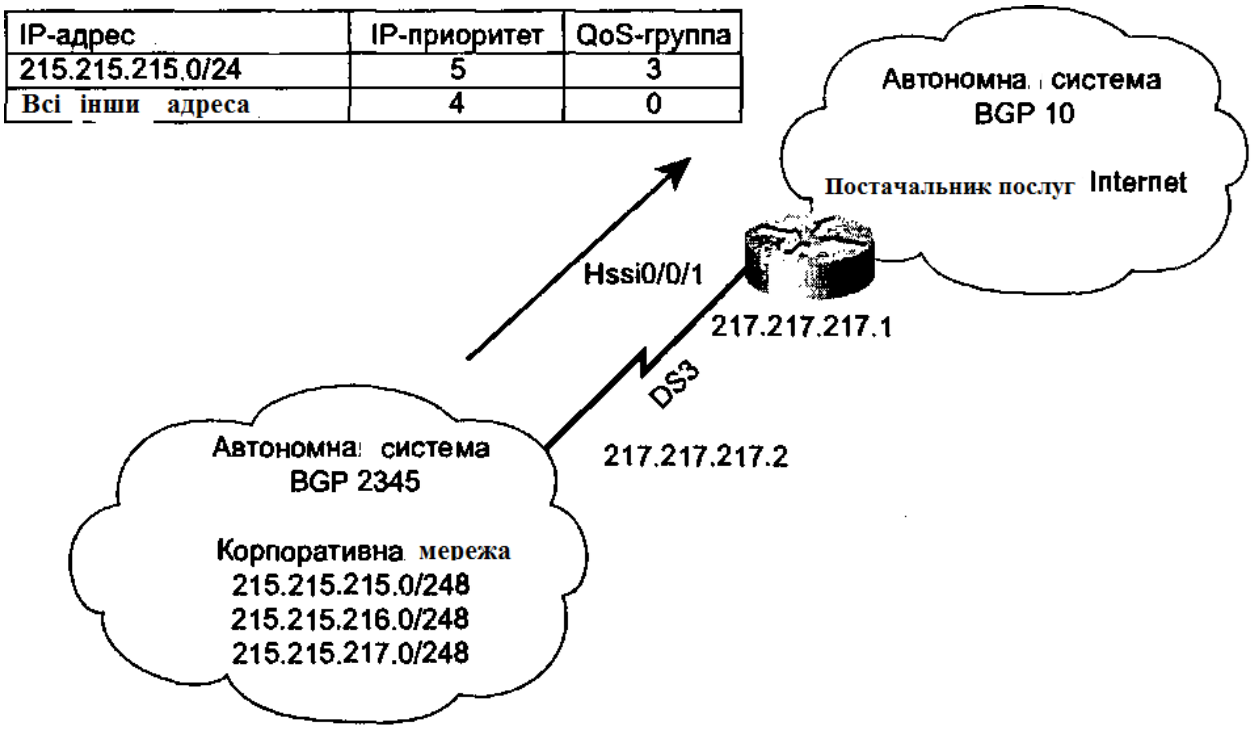


Рис. 6.10. Підключення мережі корпоративного клієнту до постачальника послуг Internet

6.3.3.3 Функція управління інтенсивністю трафіку.

Управління інтенсивністю трафіку передбачає порівняння параметрів клієнтського трафіку, що поступає в мережу, з його профілем за допомогою обмежуючої функції. І навпаки, компанія, підключена до мережі постачальника послуг, може перевіряти параметри свого вихідного трафіку з метою підтримки його інтенсивності на рівні, що задовольняє всім обмежуючим функціям постачальника послуг.

До функцій управління трафіком відносяться наступні функції:

- Дозування трафіку .

Функція дозування перевіряє трафік на відповідність заданому профілю на підставі дескриптора трафіку, такого як корзина маркерів. Результати перевірки передаються функції маркіровки трафіку, а також або функції вирівнювання трафіку, або функції відкидання пакетів – для прийняття відповідного рішення відносно "планових" і "позапланових" пакетів.

- Функція вирівнювання трафіку

Функція вирівнювання трафіку (traffic shaping) здійснює затримку пакетів шляхом їх буферизації з метою задоволення параметрів заданого профілю.

- Функція обмеження трафіку

Функція обмеження трафіку (traffic policing) здійснює відкидання всіх пакетів, що не задовольняють параметрам заданого профілю трафіку.

Послідовність обробки пакетів в мережному вузлі за допомогою функцій управління інтенсивністю наведено на рис. 6.11.

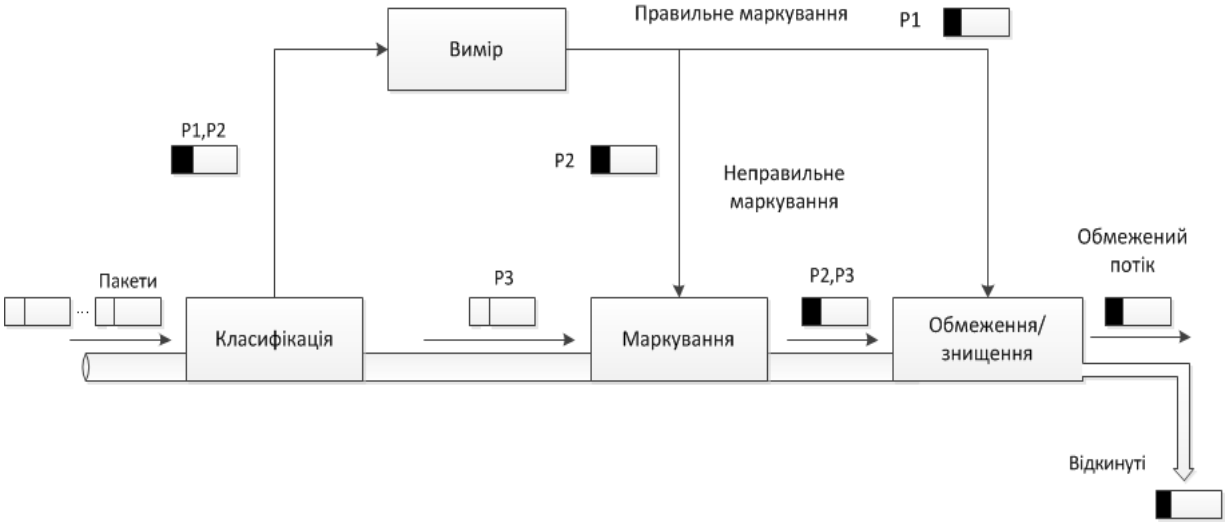


Рис. 6.11. Послідовність обробки пакетів в мережному вузлі за допомогою функцій управління інтенсивністю

Детальніше за функцію управління трафіком і механізми, що їх реалізовують, будуть розглянуті в нижче.

6.3.4 PHB-політика

Мережні вузли з підтримкою диференційованого обслуговування використовують поле DSCP в заголовку IP-пакета для визначення відповідною цьому пакету PHB-політики (PHB-per-hop behavior-покрокова поведінка).

PHB-політика може бути визначена в термінах пріоритету в наданні ресурсів по відношенню до інших PHB-політик або ж за допомогою таких вимірюваних характеристик трафіку, як затримка пакетів, рівень втрати пакетів або тремтіння трафіку. В деякій мірі PHB-політику можна розглядати як своєрідний "чорний ящик", оскільки вона визначає деяку спостережувану ззовні поведінку мережного вузла відносно пакетів, що налдходять, не нав'язуючи при цьому конкретну реалізацію.

В якості стандартної PHB-політики в *DiffServ*-мережі можна розглядати негарантовану доставку трафіку. Відповідно до архітектури диференційованого обслуговування кожній PHB-політиці рекомендується призначити певний код DSCP, проте постачальник послуг може вибрати відмінні від рекомендованих значення поля DSCP для своєї власної мережі. Рекомендоване значення поля DSCP для політики негарантованої доставки пакетів дорівнює 000 000.

PHB-політика, відповідна певному класу трафіку, залежить від цілого ряду чинників:

- інтенсивність вхідного потоку або навантаження для заданого класу трафіку. Цей параметр контролюється граничним формувачем трафіку;
- розподіл ресурсів для заданого класу трафіку. Цей параметр контролюється функціями розподілу ресурсів, реалізованими у вузлах *DiffServ* -домена;
- рівень втрати трафіку. Цей параметр залежить від політики відкидання пакетів, що проводиться у вузлах *DiffServ* -домена.

Існують дві стандартних PHB-політики – PHB-політика негайної передачі (EF PHB) і PHB-політика гарантованої доставки (AF PHB).

6.3.4.1 PHB-політика негайної передачі пакетів (Expedited Forwarding PHB – EF PHB)

Використовується для забезпечення наскрізного обслуговування пакетів у вузлах *DiffServ* -домена, характерними рисами якого є низький

рівень втрати пакетів, мала затримка, незначне тремтіння трафіку, а також гарантована смуга пропускання. Політика EF PHB застосовується для обслуговування трафіку таких застосувань, як передача голосу по мережах IP (Voice over IP – VoIP), відеоконференцій, а також для забезпечення таких послуг, як передача інформації по віртуальних каналах, що орендуються, оскільки ця послуга є двоточковим з'єднанням кінцевих вузлів *DiffServ* DiffServ -домена. Подібний тип обслуговування досить часто називають також послугами високого класу (premium service).

Одним із способів уникнути затримки пакетів, пов'язаної з виникненням великих черг, є обмеження максимальної інтенсивності вхідного потоку трафіку мінімальною інтенсивністю його вихідного потоку. PHB-політика негайної передачі пакетів передбачає установку значення інтенсивності вихідного потоку трафіку, тоді як інтенсивність вхідного потоку контролюється формувачами трафіку, реалізованими в пограничних пристроях мережі.

Оскільки відповідно до політики EF PHB вхідні пакети не повинні утворювати чергу (допускається черга дуже малого розміру), інтенсивність витікаючого потоку трафіку має бути рівній інтенсивності вхідного потоку або перевищувати її. Слід зазначити, що інтенсивність вихідного потоку (смуга пропускання) не повинна залежати від інших потоків трафіку. Як правило, інтенсивність вхідного і вихідного потоків вимірюється з інтервалами, рівними часу, який потрібний для передачі MTU-пакету (пакету максимального розміру, який може бути переданий через інтерфейс маршрутизатора) по даній лінії зв'язку.

Маршрутизатор може виділити ресурси, достатні для забезпечення певної інтенсивності вихідного трафіку для заданого інтерфейсу, шляхом використання різних функціональних реалізацій політики EF PHB. Коли йдеться про передачі трафіку через перенавантажений сегмент мережі (а це передбачає наявність великих накопичених черг), дана функціональна можливість може бути реалізована за рахунок використання різних механізмів обслуговування черг.

6.3.4.2 PHB-політика гарантованої доставки пакетів (Assured Forwarding PHB – AF PHB)

PHB-політика гарантованої доставки пакетів (AF PHB) є засобом, за допомогою якого постачальник послуг може забезпечити декілька різних

рівнів надійності доставки IP-пакетів, отриманих з DiffServ-домена клієнта. Політика AF PHB є прийнятною для більшості TCP-застосувань.

PHB-політика гарантованої доставки пакетів передбачає наявність різних рівнів обслуговування для кожного з чотирьох класів AF-трафіка. Кожному класу AF-трафіка відповідає власна черга пакетів, що дозволяє проводити ефективне управління смугою пропускання. Кожен клас AF-трафіка характеризується трьома рівнями пріоритету відкидання пакетів (низький, середній і високий), що дозволяє реалізувати механізм управління чергою за типом механізму довільного раннього виявлення (Random Early Detection – RED).

Політика AF PHB є засіб, за допомогою якого постачальник послуг може забезпечити декілька різних рівнів надійності доставки IP-пакетів залежно від значення поля DSCP.

Підіб'ємо підсумки викладеному. Область DiffServ (DS) складається з одного або більш за DS-доменів. Кожен DS-домен конфігурується з використанням значень DSCP і різних параметрів PHB. На всьому протязі IP-маршруту, по якому перемішається пакет, всі пристрої повинні підтримувати службу DiffServ. Сам DS-домен включає вхідні DS-вузли, внутрішні DS-вузли в базовій магістралі і вихідні DS-вузли. Вхідний або вихідний DS-вузол може бути граничним DS-вузлом, який сполучає два DS-домена. Зазвичай граничний DS-вузол виконує класифікацію потоків даних. Класифікатор потоків даних відносить вхідні пакети до заздалегідь визначених потоків на основі вмісту частини заголовка пакету, перевіряє їх відповідність параметрам потоку або позначає їх відповідним чином, записуючи або перезаписуючи код DSCP і поміщає в буфер для досягнення необхідної швидкості потоку або відкидає пакет в разі виникнення затору. Внутрішній вузол DiffServ забезпечує відповідну поведінку функцій PHB шляхом використання механізмів формування або вибору стратегії.

Детальніше за функцію управління трафіком і механізми, що їх реалізовують, будуть розглянуті в наступному пункті.

6.3.5 Механізми формування трафіку на кордоні мережі. Управління інтенсивністю трафіку

Навіть якщо невелике число граничних маршрутизаторів почнуть передавати трафік з інтенсивністю, що перевищує максимально допустиме значення, навантаження потоку трафіку може збільшитися настільки, що це приведе до перевантаження мережі. А зниження продуктивності мережі

неминуче приведе до неможливості забезпечення функцій якості обслуговування для всього мережного трафіку.

Управління інтенсивністю трафіку може бути досягнуте за рахунок застосування двох функцій: функції обмеження трафіку, передбаченій механізмом CAR, і функції вирівнювання трафіку (traffic shaping – TS), передбаченій однойменним механізмом.

Базовим механізмом, що забезпечує дозовану передачу трафіку є алгоритм “корзина маркерів”, причому цей алгоритм використовується як в механізмі обмеження, так і в механізмі вирівнювання трафіку.

6.3.5.1 Корзина маркерів

Корзина маркерів - механізм, що дозволяє передавати пакети, що поступають на вхідний інтерфейс мережного вузла, з швидкістю, що не перевищує адміністративно заданий поріг, але з можливістю перевищення його для коротких сплесків.

Максимальна середня швидкість відправки потоку пакетів з управляючого вузла, залежить від швидкості надходження маркерів. Число маркерів в буфері, який називається корзиною маркерів, визначає число байт даних, дозволених на передачу. Черговий пакет може бути відправлений лише при отриманні числа маркерів, достатнього для передачі даних, об'єм яких більше або дорівнює розміру пакету. Якщо дані прибувають з швидкістю, рівній швидкості вхідних маркерів, то кожен пакет має відповідні маркери і проходить чергу без затримки. Якщо дані прибувають швидше, ніж маркери, то в корзині (буфері) з часом не залишиться маркерів, що приведе до припинення передачі даних. Якщо пакети продовжують поступати, вони починають знищуватися. Дана ситуація дозволяє адміністративно обмежувати доступну смугу пропускання.

Схема “корзина маркерів” передбачає наявність трьох ключових параметрів.

- Середня інтенсивність, або погоджена швидкість передачі інформації (Committed Information Rate - CIR), біт/с. Як правило, інтенсивність трафіку не перевищує погоджену швидкість передачі інформації.
- Погоджений розмір сплеску (B_C), байт. Об'єм трафіку, на який може бути перевищений розмір корзини маркерів в окремо взятий момент часу. Інколи цей параметр називають також стандартним розміром сплеску.
- Розширений розмір сплеску (B_E), байт. “Резервний фонд”. Об'єм трафіку, на який може бути перевищений розмір корзини маркерів в екстреному випадку. Сплеск, розмір якого знаходиться між погодженим і

розширеним розміром, дозволяється, як правило, лише для дуже невеликої частини трафіку.

- Четвертий ключовий параметр - інтервал часу (time interval - TI) – залежить від середньої інтенсивності трафіку і погодженого розміру сплеску і обчислюється за формулою $TI = B_C/CIR$.

6.3.5.2 Обмеження трафіку (Traffic Policing) з використанням механізму "корзина маркерів"

Функція обмеження трафіку забезпечується механізмом узгодження швидкості доступу (Committed Access Rate — CAR). В цілому механізм CAR реалізує дві основні функції: маркіровка пакетів шляхом установки значення поля IP-пріоритету і обмеження інтенсивності трафіку.

Як функція обмеження трафіку механізм CAR не розміщує пакети в буфер і не згладжує трафік, що може привести до відкидання пакетів в моменти перевищення максимально допустимого розміру сплеску. Реалізація механізму CAR є послідовністю наступних кроків:

Крок 1. Аналіз типа трафіку, що поступає. Якщо умова співпадання трафіку не виконується (на підставі списків доступу), то вихід з процедури, інакше - перехід до наступного Кроку.

> ***Примітка.*** *Умова співпадіння трафіку може охоплювати всі пакети, або реалізується на основі списків доступу. Списки доступу визначають критерії, на відповідність яким перевіряється кожен пакет, оброблюваний роутером в точці списку доступу. Кожен критерій в списку доступу записується окремим рядком. Якщо пакет задовольняє якому-небудь критерію (IP-приоритет, MAC-адрес і так далі), то подальші перевірки його на відповідність наступним критеріям в списку - не проводяться*

Крок 2. Виклик процедури дозування трафіку "корзина маркерів". Перехід до наступного Кроку.

Крок 3. Визначення політики обробки пакетів (передача пакету, відкидання пакету).

Крок 4. Кінець процедури.

Основним засобом дозування трафіку є схема “корзина маркерів”. Реалізація цієї схеми в рамках механізму узгодження швидкості доступу (CAR) представлена на рис. 6.12. Розмір корзини маркерів (максимальне число маркерів, яке може вміщати корзина) дорівнює погодженому розміру сплеску (B_C). Реалізація алгоритму "корзини маркерів" залежить від величини розширеного розміру сплеску (B_E).

Стандартна корзина маркерів не підтримує можливість екстреного збільшення розміру сплеску. Розширений розмір сплеску для стандартної корзини маркерів завжди дорівнює погодженому розміру сплеску. В цьому випадку брак маркерів наводить до відкидання пакету. На відміну від стандартної корзини маркерів, корзина маркерів з можливістю екстреного збільшення розміру сплеску дозволяє “зайняти” недостатні маркери.

Узагальнений алгоритм "корзини маркерів" є послідовністю наступних кроків.

Крок 1. Аналіз пакету, що поступає. Порівняння числа маркерів в корзині з розміром пакету, що поступив, в байтах. Якщо маркерів більше, перехід до наступного Кроку, інакше - перехід до Кроку 3.

Крок 2. Зменшення лічильника маркерів на величину рівну розміру пакету в байтах. Передача пакету. Перехід до Кроку 1 в разі наявності трафіку, що поступає, або вихід з процедури в разі його відсутності (Крок 6).

Крок 3. Порівняння погодженого і розширеного розмірів сплеску. Якщо $B_E = B_C$ (стандартна корзина маркерів), то пакет відкидається і слідує перехід до Кроку 1. Якщо $B_E > B_C$ (корзина маркерів з можливістю екстреного збільшення розміру сплеску), то перехід до наступного Кроку.

Крок 4. Встановлюється розмір поточного боргу (actual debt - D_A) рівним недостатній кількості маркерів в даний момент. Встановлюється розмір накопиченого боргу (compounded debt - D_C) рівним сумі поточних боргів (D_A) всіх пакетів, переданих з моменту останнього відкидання. Перехід до наступного Кроку.

Крок 5. Порівняння розмірів поточного боргу D_A і накопиченого боргу D_C з розширеним розміром сплеску B_E. Якщо $D_A < B_E$ і $D_C < B_E$, то пакет передається. Перехід до Кроку 1. Якщо поточний борг $D_A > B_E$, пакети відкидаються до тих пір, поки значення D_A не повернеться в допустимі межі (поточний борг зменшується через постійні часові інтервали завдяки накопиченню маркерів і визначається сконфігурованою погодженою швидкістю передачі інформації), а значення накопиченого боргу D_C обнуляється.

Якщо $D_C > B_E$, пакет відкидається, а значення накопиченого боргу D_C обнуляється. Перехід до Кроку 1.

Крок 6. Кінець процедури.

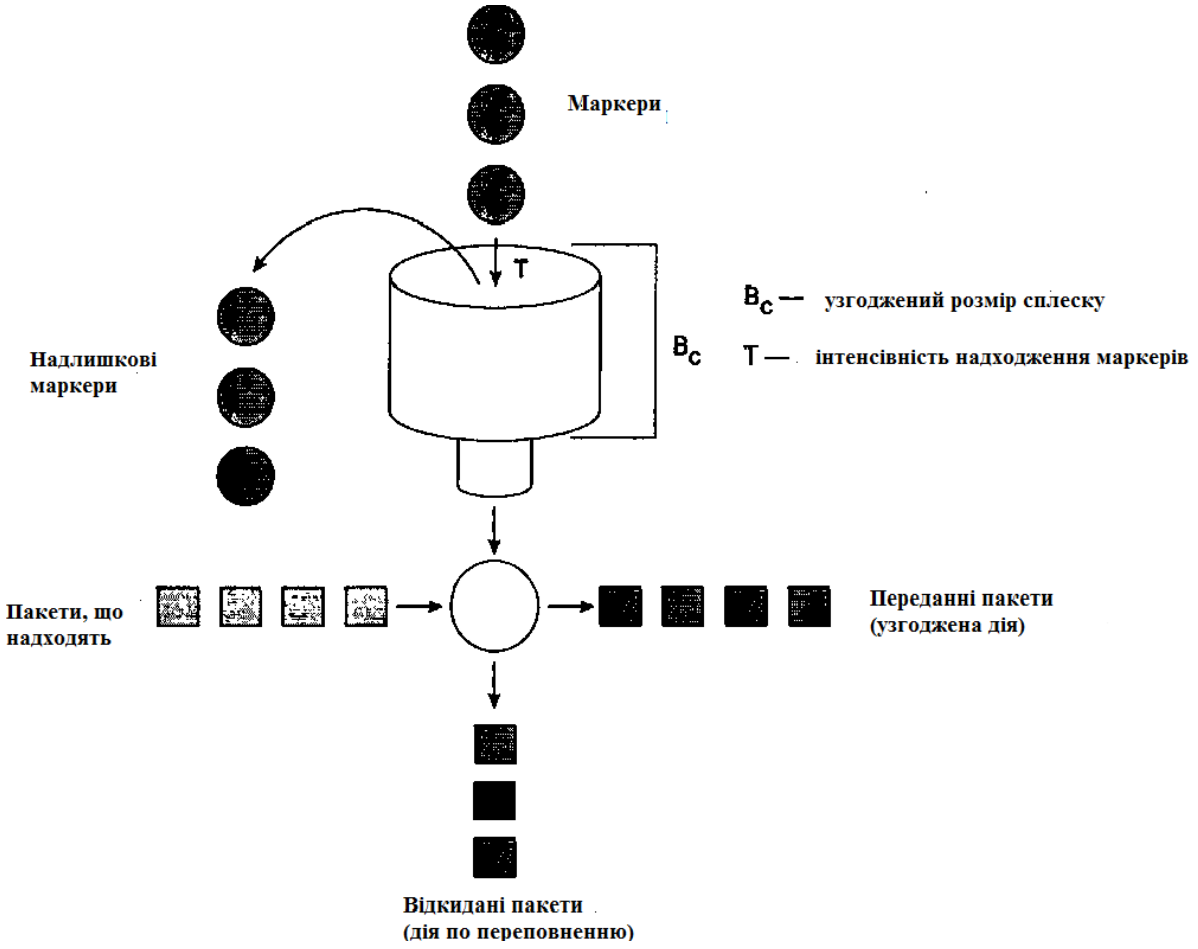


Рис. 6.12. Стандартна корзина маркерів.

Розглянемо на прикладі функціонування алгоритму корзини маркерів з можливістю екстреного збільшення розміру сплеску. Припустимо, що услід за останнім відкиданням пакету було зайнято по 100 маркерів для передачі кожного з трьох пакетів даних.

Таким чином, значення поточного боргу D_A після передачі першого, другого і третього пакетів рівне, відповідно, D_{A1}=100, D_{A2}=200 і D_{A3}=300. Накопичений борг (D_C) є сумою поточних боргів (D_A) всіх пакетів, переданих з моменту останнього відкидання. На відміну від поточного боргу (D_A), що є кількістю зайнятих маркерів з моменту останнього відкидання пакету, накопичений борг (D_C) є сумою поточних боргів всіх пакетів, для передачі яких потрібно було зайняти маркери з моменту останнього відкидання пакету.

Аналогічно попередньому прикладу, припустимо, що услід за останнім відкиданням пакету ви займали по 100 маркерів для передачі кожного з трьох пакетів даних.

Таким чином, значення нагромадженого боргу D_C після передачі першого рівне 100, після передачі другого дорівнює

$D_C = D_{A1} + D_{A2}$=100+200=300,

після передачі третього дорівнює

$D_C = D_{A1} + D_{A2} + D_{A3} = 100 + 200 + 300 = 600$

Таким чином, після передачі першого пакету (для якої потрібно було зайняти маркери) з моменту останнього відкидання величина накопиченого боргу D_C стає рівній величині поточного боргу D_A.

При втраті пакету значення нагромадженого боргу D_C обнуляється, а значення поточного боргу D_A зберігається. Наступному пакету, для передачі якого потрібно буде зайняти маркери, ставиться в відповідність нове значення накопиченого боргу D_C, рівне поточному боргу D_A. Наприклад, в тому випадку, якщо четвертий пакет буде відкинутий, наступному пакету, для передачі якого потрібно буде зайняти маркери (передбачимо, 100), буде поставлено у відповідність значення накопиченого боргу

$D_C = D_{A4} = 300+100=400$. (на відміну від накопиченого боргу D_C, значення поточного боргу D_A не обнуляється після відкидання пакету).

Якщо поточний борг D_A перевищує розширену межу, пакети відкидаються до тих пір, поки значення D_A не повернеться в допустимі межі (нагадаємо, що зменшення поточного боргу проводиться за рахунок накопичення маркерів).

Потреба у використанні корзини з можливістю збільшення розміру екстреного сплеску обумовлюється такою вельми небажаною властивістю стандартної корзини маркерів, як “відкидання хвоста” (tail-drop). Корзина маркерів з можливістю збільшення розміру екстреного сплеску забезпечує поступове відкидання пакетів, характерніше для алгоритму довільного раннього виявлення (Random Early Detection - RED). Якщо для передачі пакету, що знов прийшов, потрібно зайняти деяке число маркерів, проводиться порівняння розширеного розміру сплеску B_E і накопиченого боргу D_C. Якщо D_C більше, ніж B_E, пакет відкидається, а значення накопиченого боргу D_C обнуляється. Інакше пакет передається, при цьому поточний борг D_A збільшується на число зайнятих маркерів, а нагромаджений борг D_C - на величину, рівну оновленому значенню поточного боргу D_A.

Слід зазначити, що коли пакет відкидається унаслідок браку маркерів (тобто коли число доступних маркерів менше розміру пакету в байтах), корзина не спустошується (іншими словами, відкидання пакетів не призводить до зменшення межі сплеску або межі інтенсивності трафіку).

Необхідно пам'ятати, що погоджена швидкість передачі даних (CIR) – це величина, вимірювана в байтах в секунду. У свою чергу сплеск трафіку виражається в байтах. Поточний розмір сплеску зберігається в лічильнику сплеску. Значення лічильника сплеску може бути як менше,

так і більше, ніж погоджений розмір сплеску B_C. Коли значення лічильника сплеску перевищує B_C, воно дорівнює сумі розміру погодженого сплеску і поточного боргу:

$$B_C + D_A$$

У момент вступу нового пакету значення лічильника сплеску оновлюється, як показано на рис. 6.13. У разі, коли значення лічильника сплеску знаходиться між погодженим B_C і розширеним B_E розмірами сплеску, імовірність дії з переповнювання може бути приблизно розрахована по наступній формулі:

$$(\text{Лічильник сплеску} - B_C)/(B_E - B_C)$$

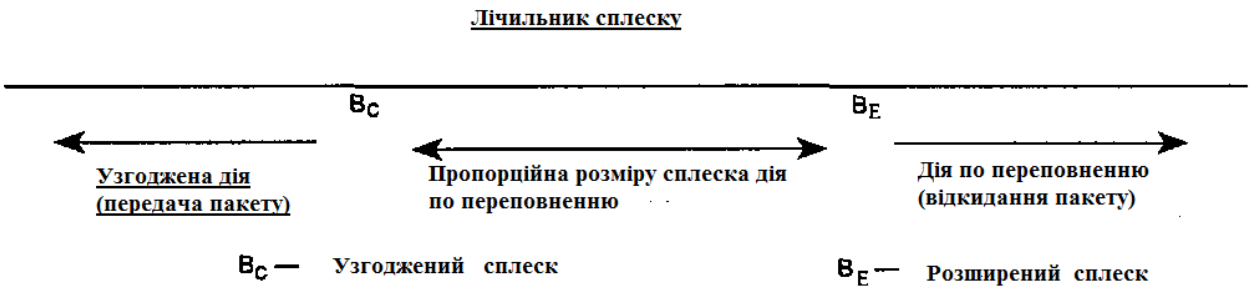


Рис. 6.13. Вибір відповідної дії на основі лічильника сплеску

На рис.6.14 представлений графік імовірності відкидання пакету механізмом CAR з врахуванням запропонованої апроксимації.

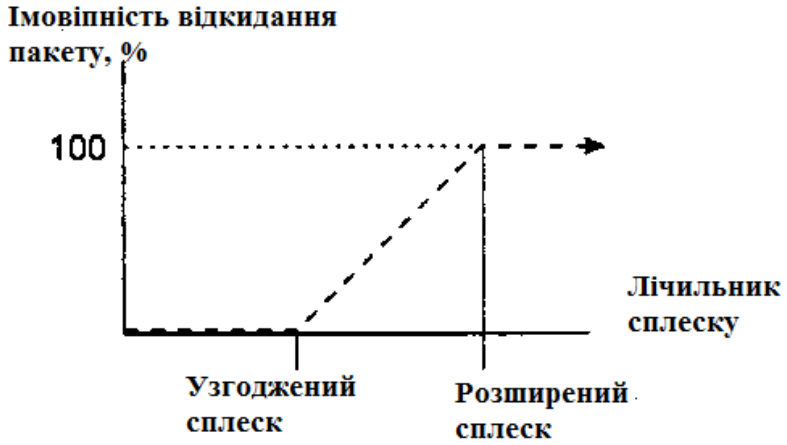


Рис. 6.14. Графік імовірності відкидання пакету механізмом CAR

Лінійне зростання імовірності відкидання пакету механізмом CAR на відрізку між погодженим і розширеним розмірами сплеску нагадує лінійне зростання імовірності відкидання пакету механізмом RED на відрізку між мінімальним і максимальним пороговим значенням.

Будемо вважати, що під погодженою дією і дією з переповнювання мається на увазі відповідно передача і відкидання пакету. Насправді ж погоджена дія і дія з переповнювання може бути визначена безліччю різних способів, які визначаються політикою для погодженої дії і дії з переповнювання для обмеження інтенсивності трафіку.
Наприклад,

- передати пакет;
- відкинути пакет;
- встановити значення поля IP-пріоритету і передати пакет;
- встановити значення поля IP-пріоритету і продовжити перегляд списку операторів з обмеження інтенсивності трафіку;
- встановити значення поля QoS-групи і передати пакет;
- встановити значення поля QoS-групи і продовжити перегляд списку операторів з обмеження інтенсивності трафіку.

Слід зазначити, що типовий оператор обмеження інтенсивності трафіку, в якому погоджений B_C і розширений B_E розміри сплеску рівні між собою, виключає можливість лінійного зростання імовірності відкидання пакету на якій-небудь ділянці.

Зазвичай реалізація механізму узгодження швидкості доступу (CAR) накладає наступні обмеження на параметри корзини пакетів.

- Крок збільшення інтенсивності передачі трафіку (біт/с) дорівнює 8 Кбіт/с, а найменше значення погодженого і розширеного розміру сплеску - 8000 байт.
- Мінімальне значення погодженого розміру сплеску (B_C) дорівнює відношенню інтенсивності передачі трафіку (біт/с) до 2000. Найменше значення погодженого розміру сплеску дорівнює 8000 байт (наприклад, CIR=30000000 біт/с., $B_C = B_E = 15000$ байт)
- Розширений розмір сплеску B_E завжди дорівнює погодженому розміру сплеску B_C або більше його.

6.3.5.3 Вирівнювання трафіку (Traffic Shaping) з використанням механізму "корзина маркерів"

Вирівнювання трафіку (traffic shaping - TS) є механізмом згладжування потоку трафіку, що поступає на інтерфейс, з метою недопущення перевантаження каналу і задоволення вимог постачальника послуг. Відповідно до механізму TS інтенсивність пульсуючого трафіку вирівнюється до погодженої швидкості передачі інформації (CIR) шляхом постановки в чергу (буферизації) пакетів, інтенсивність передачі яких

перевищила середнє значення. Буферизовані пакети передаються у міру накопичення достатнього числа маркерів. Передача поставлених в чергу пакетів планується механізмом обслуговування черг “першим прийшов, першим обслужений” (first-in, first-out – FIFO) або зваженим механізмом рівномірного обслуговування черг (Weighted Fair Queuing – WFQ). Операційна модель механізму вирівнювання трафіку схематично представлена на рис. 6.15.

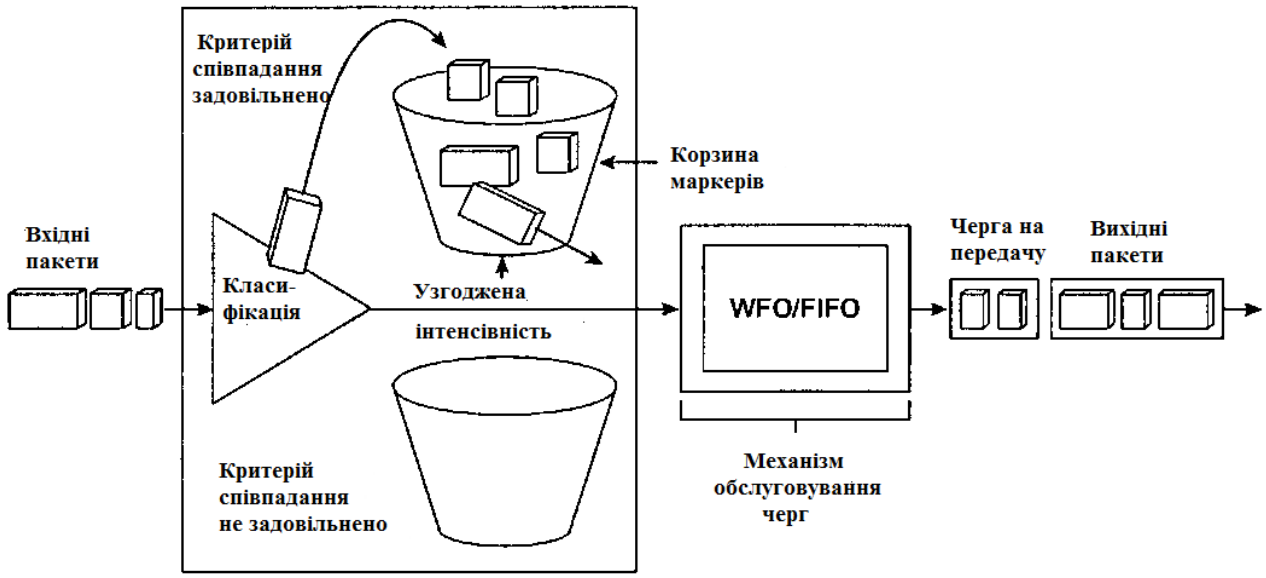


Рис. 6.15. Операційна модель механізму вирівнювання трафіку

6.3.5.3 Дозування трафіку (інструмент виміру трафіку) з використанням механізму "корзина маркерів"

Функція дозування перевіряє трафік на відповідність заданому профілю на підставі дескриптора трафіку, такого як корзина маркерів. Результати перевірки передаються функції маркіровки трафіку, а також або функції вирівнювання трафіку, або функції відкидання пакетів – для прийняття відповідного рішення.

Як інструмент дозування трафіку механізм TS використовує корзину маркерів, яка застосовується для перевірки пакетів, що поступають на вхідний інтерфейс мережного вузла, на відповідність заданому профілю.

Максимальний розмір корзини маркерів дорівнює сумі розмірів погодженого (B_C) і розширеного (B_E) сплесків. Корзина поповнюється маркерами, кількість яких дорівнює розміру погодженого сплеску (B_C), через кожен інтервал часу

$$T= B_C/ CIR$$

де CIR є погодженою середньою інтенсивністю потоку трафіку. Коли корзина стає повною, надлишкові маркери, що знов прибувають, відкидаються. Для кожного пакету, що обробляється відповідно до

механізму TS, з корзини виймається кількість маркерів, рівне розміру пакету в байтах. Якщо для передачі пакету в корзині знайшлася достатня кількість маркерів, пакет передається, а розмір корзини зменшується на кількість маркерів, що дорівнює розміру переданого пакету. Інакше пакет маркірується як не задовольняючий заданому профілю і ставиться в чергу для подальшої передачі. На рис. 6.16 наведена реалізація алгоритму “корзина маркерів” для механізму вирівнювання трафіку.

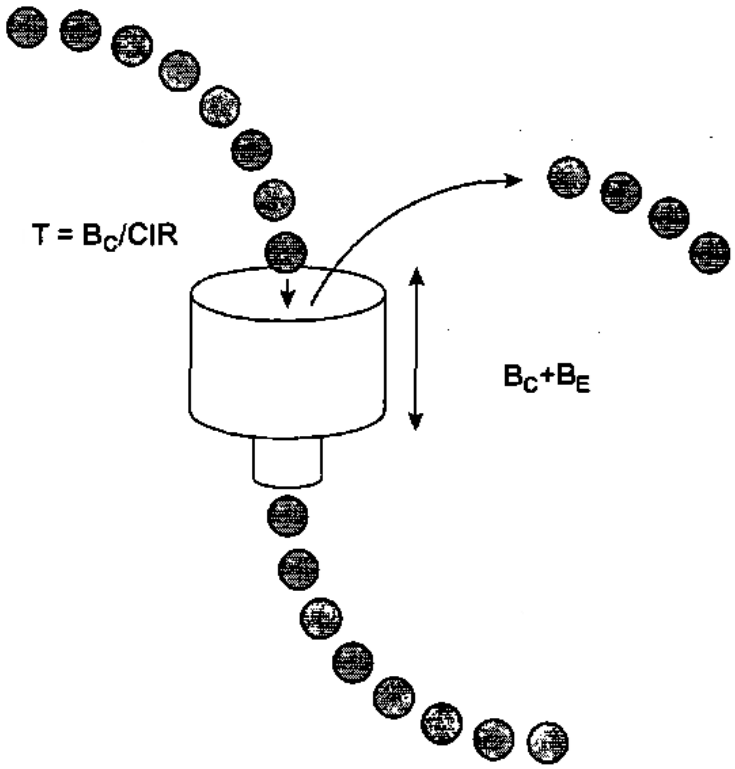


Рис. 6.16. наведена реалізація алгоритму “корзина маркерів” для механізму вирівнювання трафіку

Підсумовуючи вищенаведене, можна зробити такі висновки.

Формувачі трафіку на границі мережі виконують наступні функції якості обслуговування: класифікація пакетів, маркіровка пакетів і управління інтенсивністю трафіку.

Головною метою класифікації пакетів, що проводиться на границі мережі, є створення передумови для диференційованого обслуговування пакетів усередині мережі. Класифікація пакетів є необхідною умовою для ідентифікації різних класів трафіку залежно від необхідного рівня обслуговування. IP-пакет може бути класифікований на підставі одного або декількох полів заголовка. Після віднесення пакету до певного класу він маркірується за допомогою установки відповідного значення поля IP-пріоритету, поля DSCP або поля QoS-групи.

Управління інтенсивністю трафіку на границі мережі – це необхідна умова існування достатньої кількості ресурсів і забезпечення функцій якості обслуговування усередині базової мережі. Для обмеження інтенсивності трафіку, що перевищує задану межу, використовується механізм узгодження швидкості доступу (CAR).

Механізм CAR допускає пересилку деякого надлишкового об'єму трафіку з лінійним ростом інтенсивності, проте після досягнення порогового значення всі надлишкові пакети відкидатимуться. Механізм вирівнювання трафіку (TS) “згладжує” трафік шляхом буферизації пакетів, які потім пересилаються з погодженою інтенсивністю.

Механізм TS є більш дружнім для TCP, чим механізм CAR, оскільки відкидання пакетів здатне привести до звуження вікна потоку TCP до мінімального значення , що, у свою чергу, може стати причиною падіння інтенсивності потоку TCP нижче за допустиме значення. Підібравши належним чином параметри сплеску, що відрізняються в кожній реалізації протоколу TCP, можна забезпечити умови підвищення інтенсивності TCP-потоку аж до погодженої швидкості передачі інформації.

6.3.6 PHB-політика розподілу ресурсів - механізми обслуговування черг

У моменти перевантаження мережі розподіл ресурсів для окремого потоку трафіку обумовлюється порядком обслуговування поставлених в чергу пакетів. Порядок обслуговування поставлених в чергу пакетів визначає наступний пакет, який буде витягнутий з черги.

Традиційним для Internet механізмом обслуговування черг є механізм “першим прийшов, першим обслужений” (first-in, first-out — FIFO), відповідно до якого пакети передаються в тому порядку, в якому вони були поставлені у вихідну чергу. Не дивлячись на те що механізм FIFO досить простий і його легко реалізувати, він не здатний проводити відмінність між декількома потоками трафіку. Отже, механізм FIFO не може забезпечити його пріоритетну по відношенню до інших потоків обробку.

Зважений механізм рівномірного обслуговування черг (Weighted Fair Queuing - WFQ) є механізмом обслуговування черг з врахуванням приналежності пакетів до того або іншого класу трафіку. Відповідно до механізму WFQ кожному потоку трафіку призначається певна вага, яка обумовлює частоту обслуговування пакетів даного потоку. Механізм WFQ підтримує пріоритетну обробку потоків з великою вагою, а також захист і рівномірне обслуговування потоків з однаковою вагою шляхом вживання максимінної схеми рівномірного розподілу ресурсів (max-min fair-share,

allocation scheme). Ми розглянемо максимінну схему рівномірного розподілу ресурсів і її реалізацію у вигляді механізму рівномірного обслуговування черг (Fair Queuing – FQ). Далі розглянемо модифікований зважений алгоритм кругового обслуговування (Modified Weighted Round Robin – MWRR) і модифікований алгоритм кругового обслуговування з дефіцитом (Modified Deficit Round Robin - MDRR).

6.3.6.1 Алгоритм обслуговування черг FIFO

FIFO є механізмом обслуговування черг, відповідно до якого порядок постановки пакетів в чергу збігається з порядком їх витягання з черги для обробки (передачі). Черга механізму FIFO схематично представлена на рис. 6.17.

Рис. 6.17. Черга FIFO

Відповідно до механізму обслуговування FIFO порядок постановки пакетів в чергу збігається з порядком їх витягання з черги. На сьогоднішній день механізм FIFO є найбільш поширеним механізмом обслуговування черг, що застосовується в маршрутизаторах. Його реалізація відрізняється своєю простотою. На жаль, механізм FIFO не має засобів диференціювання потоків трафіку і, отже, не може виділити пріоритетні потоки. Більш того, механізм FIFO не здатний забезпечити рівномірне обслуговування потоків трафіку з однаковим пріоритетом і захистити їх від пригнічення потоками з нерівномірною інтенсивністю. Останні можуть відібрати частину ресурсів в потоків, що мають постійну інтенсивність і що обслуговуються наскрізними адаптивними схемами управління потоком, такими, як схема управління динамічним вікном протоколу TCP (Transmission Control Protocol – протокол управління передачею). Відповідно до механізму FIFO потоки трафіку обслуговуються майже пропорційно їх інтенсивності. Подібна схема обслуговування черг не є рівномірною, оскільки вона допускає переважання потоків високої інтенсивності над всіма іншими потоками трафіку. Будь-який же рівномірний алгоритм обслуговування черг

забезпечує захист від потоків з високою інтенсивністю за своєю природою.

Далі розглянемо алгоритм, за допомогою якого можна забезпечити рівномірне обслуговування черг.

6.3.6.2 Максимінная схема рівномірного розподілу ресурсів

Схемою рівномірного розподілу ресурсів, що отримала широке визнання, є максимінна схема рівномірного розподілу ресурсів (max-min fair-share allocation scheme).

Різні користувачі можуть пред'являти різні вимоги до ресурсів. Отже, існує можливість класифікації користувачів в порядку зростання їх вимог до ресурсів.

Основними принципами максимінної схеми рівномірного розподілу ресурсів є:

1) Ресурси розподіляються в порядку зростання вимог.
2) Користувач не може отримати об'єм ресурсів, що перевищує його потреби.
3) Ресурси розподіляються рівномірно між користувачами з незадоволеними вимогами.

Розглянемо алгоритм максимінної схеми рівномірного розподілу ресурсів у вигляді послідовності кроків. Вихідними даними для цієї задачі є відомий загальний об'єм доступного ресурсу і вимоги до ресурсу з боку користувачів.

Крок 1. Визначити, вимога якого користувача до ресурсу є найменшою. Ця вимога отримує об'єм ресурсу, рівний відношенню всього запасу ресурсу до загального числа користувачів.

Крок 2. Визначити об'єм доступного ресурсу, що залишився.

Крок 3. Перевірити, чи не перевищує об'єм ресурсу, отриманий користувачем, необхідне значення. Якщо так, то "зайвий" ресурс додається до того, об'єма доступного ресурсу, який залишився.

Крок 4. Визначити наступного користувача з найменшим за об'ємом запрошуваним ресурсом. Ця вимога отримує об'єм ресурсу, визначуваний таким чином:

$$V_k = \frac{V_\sum - V_P}{N},$$

де V_k - об'єм ресурсів, що надається користувачеві; $V_\sum$ - весь запас доступних ресурсів; V_P – об'єм вже розподілених ресурсів); N – число користувачів, яким все ще потрібні ресурси.
Потім Кроки 2-4 повторюються до тих пір, поки всі вимоги не будуть задоволені.

Розглянемо функціонування цього алгоритму на конкретному прикладі. Припустимо, що загальний об'єм доступного ресурсу дорівнює 14 одиницям. Вимоги до ресурсу користувачів A, B, C, D і E складають 2, 2, 3, 5 і 6 одиниць, відповідно. Розподіл ресурсу починається з джерела з найменшими вимогами, яке отримує об'єм ресурсу, рівний відношенню всього запасу ресурсу до загального числа користувачів. Таким чином, у випадку, що розглядається нами, користувачам A і B буде надано 14/5 = 2.8 одиниць ресурсу, тобто вимоги користувачів A і B задовольняються в повному об'ємі, оскільки вони не перевищують значення, отриманого в результаті рівномірного розподілу ресурсів між всіма користувачами. Навпаки, вимоги користувачів A і B складають всього лише 2 одиниці ресурсу. В цьому випадку надлишковий ресурс об'ємом 1.6 одиницями (по 0.8 одиниць з кожного користувача) повертається в загальний резерв доступного ресурсу. Таким чином, тепер об'єм доступного ресурсу складає 14-4=10 одиниць. Залишилися три незадоволені вимоги від трьох користувачів C, D і E. На наступному кроці ресурс, що залишився, рівномірно розподіляється між користувачами C, D і E. Кожному з них може бути надано по 10/3=3.33 одиниць ресурсу. Таким чином, на цьому кроці в повному об'ємі задовольняється лише вимога користувача C як та, що не перевищує значення, яке було отримано в результаті розподілу (необхідне 3, а отримане 3.33). Надлишкові 0.33 одиниць ресурсу повертаються в загальний резерв доступного ресурсу, який тепер складає 7 одиниць ресурсу. В результаті наступного розподілу кожен з користувачів (D і E) отримує по 7/2=3.5 одиниць ресурсу, що недостатньо для покриття їх потреб, об'єм незадоволених вимог яких складає 1.5 і 2.5 одиниць, відповідно.

Представлений вище спосіб розподілу ресурсів отримав назву максимінної схеми рівномірного розподілу ресурсів. Всі користувачі з незадоволеними вимогами (тобто з вимогами, об'єм яких перевищує їх максимінну рівномірну долю) отримують рівні об'єми ресурсів. Максимінна схема рівномірного розподілу ресурсів отримала свою назву у зв'язку з тим, що користувач з незадоволеними вимогами отримує максимум з можливих мінімальних рівномірних доль.

Максимінна схема рівномірного розподілу ресурсів, в якій кожному користувачеві призначається певна вага, отримала назву зваженої макси-

мінної схеми рівномірного розподілу ресурсів (weighted max-min fair-share allocation scheme). Відповідно до зваженої максиминной схеми рівномірного розподілу ресурсів кожному користувачеві виділяється рівномірна доля ресурсів, пропорційна його вазі.

6.3.6.3 Узагальнена схема розподілу процесорного часу

При обробці потоків трафіку, передаваного по методу негарантованої доставки (а також всіх інших рівноважних класів трафіку), повинна застосовуватися схема, що забезпечує справедливе обслуговування за типом максимінної схеми рівномірного розподілу ресурсів. Саме такий схемою і є узагальнена схема розподілу процесорного часу (Generalized Processor Sharing - GPS).

Відповідно до схеми GPS кожен потік трафіку розташовується у власній логічній черзі, після чого нескінченно малий об'єм даних з кожної непорожньої черги обслуговується за круговим принципом. Необхідність обробки нескінченно малого об'єму даних на кожному крузі обумовлена вимогою обслуговування всіх непорожніх черг на будь-якому кінцевому часовому інтервалі. Таким чином, схема GPS є справедливою у будь-який момент часу.

Якщо ж всім потокам трафіку призначити вагу, то об'єм даних потоку, що обробляється на кожному крузі, буде пропорційний його вазі. Подібне розширення схеми GPS фактично є зваженою максимінною схемою рівномірного обслуговування.

Не дивлячись на те що GPS є ідеальним втіленням максимінної схеми рівномірного розподілу ресурсів, подібна модель не може бути реалізована на практиці. Таким чином, до алгоритму обслуговування черг, придатного для практичного використання, висуваються дві вимоги: він має бути як можна ближчою апроксимацією схеми GPS і має бути таким, що реалізовується на практиці.

6.3.6.4 Зважений алгоритм рівномірного обслуговування черг (WFQ) на основі обчислення порядкового номера пакету

Зважений алгоритм рівномірного обслуговування черг на основі обчислення порядкового номера пакету імітує роботу GPS-сервера, обслуговуючого в окремий момент часу 1 байт даних. Алгоритм WFQ досить добре справляється з обробкою пакетів змінної довжини, оскільки

йому не потрібно знати заздалегідь середній розмір пакету в потоці. Основою алгоритму WFQ є алгоритм FQ, відповідно до якого всі потоки трафіку розглядаються як рівні між собою, – тобто як потоки з однаковою вагою.

Алгоритм FQ моделює схему GPS шляхом обчислення порядкового номера кожного отриманого пакету. По суті, порядковий номер пакету визначає відносний порядок обробки пакетів.

Для того, щоб зрозуміти механізм моделювання схеми GPS, введемо змінну і назвемо її лічильником циклів (round number). Значення лічильника циклів визначає кількість виконаних циклів побайтового планувальника кругового обслуговування в заданий момент часу. Обчислення порядкового номера пакету залежить від лічильника циклів найбезпосереднішим чином.

Розглянемо функціонування алгоритму на конкретному прикладі.

З метою наочної ілюстрації способу моделювання схеми GPS за допомогою алгоритму FQ розглянемо три потоки трафіку, A, B і C, розміри пакетів яких складають 128, 64 і 32 байт, відповідно. Пакети поступають один за іншим на завантажений FQ-сервер в порядку Al, A2, A3, B1, C1. Першим на FQ-сервер поступає пакет A1, потім — пакет A2 і так далі.

Назвемо потік активним (active), якщо хоч би один з пакетів, що належать цьому потоку, знаходиться в очікуванні обслуговування; інакше назвемо потік пасивним (inactive).

Припустимо, що системою FQ був отриманий пакет A1, що належить пасивному потоку трафіку. Повна обробка 128- байтового пакету побайтовим планувальником кругового обслуговування займе 128 циклів. Якщо на момент отримання пакету A1 значення лічильника циклів дорівнювало 100, то після повної передачі пакету A1 це значення стане рівним

$$100 + 128 = 228.$$

Звідси порядковий номер пакету, що належить пасивному потоку (на момент попадання в чергу немає жодного байта, що належить цьому потоку, в черзі), розраховується як сума лічильника циклів і розміру пакету в байтах. По суті, порядковий номер пакету є номером циклу, в який здійснюється передача останнього байта пакету. Оскільки насправді планувальник за один раз проводить передачу всього пакету, а не його одного байта, він обслуговує весь пакет незалежно від того, чи порівнявся лічильник циклів з порядковим номером пакету.

Коли система FQ отримає пакет A2, він вже належатиме активному потоку трафіку (оскільки в черзі присутні пакети, що належать потоку трафіку A)

завдяки наявності в черзі пакету A1 з порядковим номером 228. Порядковий номер пакету A2 дорівнює

$$228 + 128 = 356,$$

оскільки він має бути переданий після пакету A1.

Звідси, порядковий номер пакету, що належить активному потоку, розраховується як сума найбільшого порядкового номера пакету, поставленого в чергу цього потоку, і розміру пакету в байтах.

Аналогічним чином, пакету A3 призначається порядковий номер

$$356 + 128 = 484.$$

Оскільки пакети B1 і C1 належать пасивному потоку трафіку (ні пакетів трафіку B, ні пакетів трафіку C до цих пір в черзі не було), їх порядкові номери дорівнюють (100 + 64)= 164 і (100 + 32)= 132, відповідно.

Нижче приведені формули, по яких проводиться розрахунок порядкового номера пакету (Sequence Number — SN) залежно від його приналежності активному або пасивному потоку трафіку.

Для пакетів, що належать пасивному потоку трафіку

порядковий номер = розмір пакету в байтах + значення лічильника циклів на момент надходження пакету (значення лічильника циклів дорівнює порядковому номеру останнього обслуженого пакету, тобто порядковому номеру пакету, який передається зараз).

Для пакетів, що належать активному потоку трафіку

порядковий номер = розмір пакету в байтах + значення найбільшого порядкового номера пакету, поставленого в чергу цього потоку.

На рис. 6.18 схематично представлені черги пакетів з відповідними їм (пакетам) порядковими номерами.

GPS-планувальник завершить обслуговування пакету A1 на 228-м циклі. Нагадаємо, що порядковий номер пакету визначає черговість обробки пакетів планувальником. В даному випадку планувальник FQ обслуговує пакети в такому порядку: C1, B1, A1, A2, A3.

Лічильник циклів використовується виключно для обчислення порядкового номера пакетів, що належать новим (пасивним) потокам трафіку. Порядковий номер пакетів, що належать активним потокам трафіку, розраховуються з врахуванням найбільшого порядкового номера пакету, поставленого в чергу цього потоку. Таким чином, якщо пакет A4 буде прийнятий до обслуговування пакету A3, то його порядковий номер дорівнюватиме

$$(484 + 128) = 612.$$

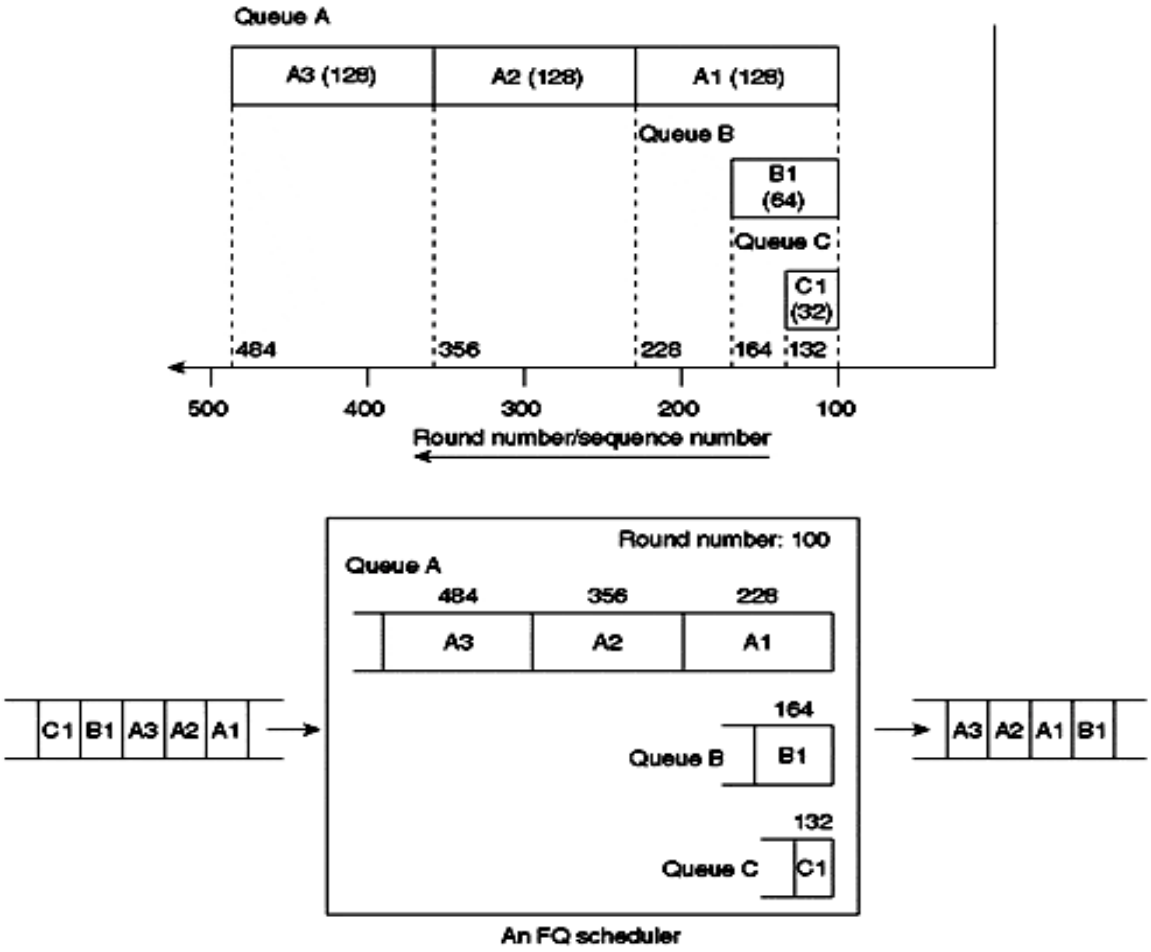


Рис. 6.18. Приклад моделювання побайтового GPS -планировщика кругового обслуговування за допомогою алгоритму FQ

Слід зазначити, що лічильник циклів оновлюється при передачі кожного чергового пакету, при цьому його нове значення дорівнює порядковому номеру пакету, який передається.

Таким чином, якщо 32-байтовий пакет D1, що належить новому потоку трафіку, буде прийнятий у момент передачі пакету A1, значення лічильника циклів дорівнюватиме 228, а порядковий номер пакету D1 (228 + 32)= 260. Оскільки порядковий номер пакету D1 менше порядкових номерів пакетів A2 і A3, він буде переданий раніше цих пакетів. Зміна в порядку обслуговування пакетів схематично змальована на мал. 6.19.

Досить типовою є ситуація, в якій одні потоки трафіку розглядаються як пріоритетніші в порівнянні з іншими. Планувальник повинен віддавати подібним потокам перевагу перед іншими, менш важливими, потоками трафіку. Цього можна досягти, призначивши кожному потоку вагу, пропорційно якому і обслуговуватиметься потік.

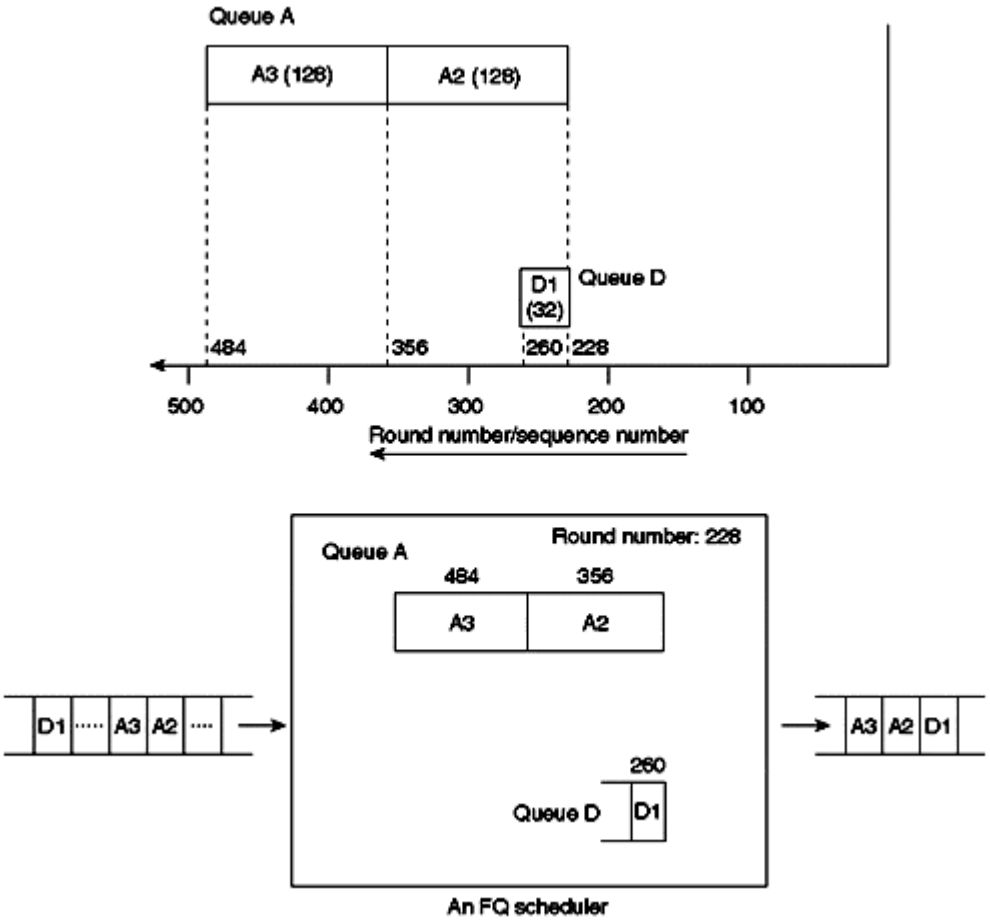


Рис. 6.19. Зміна в порядку обслуговування пакетів, викликана надходженням пакету D1 у момент передачі пакету A1

Таке розширення алгоритму рівномірного обслуговування черг (FQ) отримало назву зваженого алгоритму рівномірного обслуговування черг (WFQ) на основі потоку.

6.3.6.5 Зважений алгоритм рівномірного обслуговування черг (WFQ) на основі потоку

Відповідно до механізму WFQ вага пакету визначається на підставі значення поля IP-пріоритету і визначається по наступній формулі:

$$Вага = \frac{4096}{IP\ приоритет + 1}$$

Примітка.

*Існують інші версії приведеної формули. У пізніших версіях операційної системи в устаткуванні фірми Cisco чисельник умножається ще на 8 (4096*8=32768) . Таким чином, формула набуває вигляду:* $Вага = \frac{32768}{IP\,приоритет + 1}$.

Залежність ваги пакету від значення поля IP-пріоритету і байта типа обслуговування (Type of Service — ToS) показана в табл. 6.6.

Таблиця 6.6. Залежність ваги пакету від значення поля IP-пріоритету

		Вага	
IP-пріоритет	Значення байта ToS	Версія 1	Версія 2
0	0 (0x00)	4096	32768
1	32 (0x20)	2048	16384
2	64 (0x40)	1365	10920
3	96 (0x60)	1024	8192
4	128 (0x80)	819	6552
5	160 (0xA0)	682	5456
6	192 (0xC0)	585	4680
7	224 (0xE0)	512	4096

Алгоритм WFQ використовує два параметри для визначення порядкового номера пакету. Подібно до алгоритму FQ, одним з параметрів є розмір пакету в байтах. До того ж алгоритм WFQ враховує призначену пакету вагу. Порядковий номер пакету дорівнює добутку його розміра в байтах і ваги пакету. Це і є єдина відмінність алгоритмів WFQ і FQ.

Перед обчисленням порядкового номера пакету лічильник циклів умножається на вагу пакету. Іншими словами, відповідно до алгоритму WFQ порядковий номер пакету визначає відносне положення пакету в WFQ-планувальникі, а лічильник циклів – порядковий номер останнього обслуженого WFQ- планувальником пакету.

Розглянемо функціонування алгоритму на тому ж самому прикладі, який ми розглядали для алгоритму WFQ на основі обчислення порядкового номера.

Припустимо, що пакети потоку А мають пріоритет 5, а пакети потоків В і С – пріоритет 0. Відповідно до алгоритму WFQ пакетам потоку А призначається вага 683, а пакетам потоків В і З — вага 4096. Всі параметри потоків, що розглядаються в даному прикладі, приведені в таблиці. 6.7.

Таблиця 6.7. Приклад роботи зваженого алгоритму рівномірного обслуговування черг (WFQ) на основі потоку

Черга	Розмір	Пріоритет	Вага = 4096/(Пріоритет + 1)
A	128	5	683
B	64	0	4096
C	32	0	4096

Порядковий номер пакету A1 дорівнює

$$100 + (683 \cdot 128) = 87524$$

Аналогічним чином розраховуються порядкові номери пакетів A2, A3, B1 і C1, рівні:

- для A2

$$(683 \cdot 128) + 87524 = 174948$$

- для A3

$$(683 \cdot 128) + 174948 = 262372$$

-для B1

$$(4096 \cdot 64) + 100 = 262244$$

для C1

$$(4096 \cdot 32) + 100 = 131172$$

Таким чином, планувальник WFQ обслуговує отримані пакети в порядку A1, C1, A2, B1, A3, як показано на мал. 6.20.

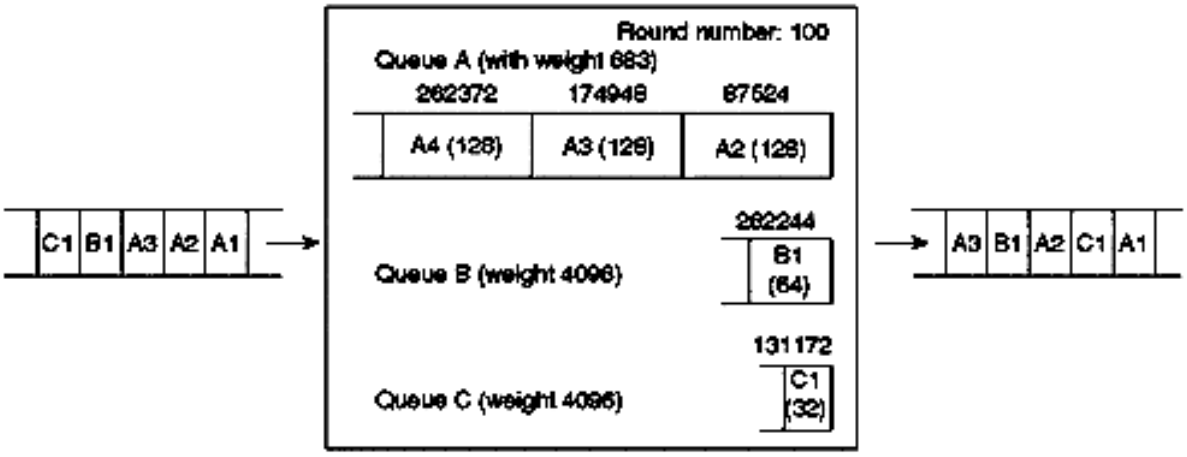


Рис. 6.20. Ілюстрація роботи зваженого алгоритму рівномірного обслуговування черг на основі потоку

Слід зазначити, що за допомогою алгоритму WFQ можна встановити вищий пріоритет потоку A, проте неможливо забезпечити рівномірне обслуговування потоків B і C. Фактично планувальник WFQ моделює максимінну зважену схему GPS.

Якщо пакети A4 і D1 (новий потік з пріоритетом 0 і розміром пакету 32 байт) будуть отримані після обробки планувальником WFQ пакету A1, їм будуть призначені порядкові номери:

- для A4

$$(683 \cdot 128) + 262372 = 349796$$

- для D1

$$(4096 \cdot 32) + 87524 = 218596$$

Міркування з приводу обчислення порядкових номерів пакетів A4 і D1 для раніше наведеного алгоритму (WFQ з порядковим номером), можуть бути віднесені і до алгоритму WFQ на основі потоку. Тепер планувальник WFQ обслуговуватиме пакети, що залишилися, в наступному порядку: C1, A2, D1, B1, A3 і A4 (рис. 6.21).

Пакет D1 був отриманий практично відразу ж після обробки планувальником WFQ пакету A1. Відзначимо, що пакет D1 буде переданий перед пакетами A3 і A4, які були поставлені в чергу раніше.

Примітка

Порядковий номер пакету, що поступив на інтерфейс, обчислюється лише в разі перевантаження вихідного інтерфейсу в результаті переповнювання буфера апаратної черги. Якщо ж вихідний інтерфейс не перенавантажений, застосовується алгоритм обслуговування черг FIFO, відповідно до якого вхідний пакет просто ставиться в апаратну чергу передачі вихідного інтерфейсу.

Довжина апаратної черги передачі інтерфейсу визначає максимальну затримку черги трафіку масштабу реального часу для планувальника WFQ. Перш ніж почати передачу пакетів трафіку масштабу реального часу (наприклад, голосового трафіку), маршрутизатор повинен передати всі пакети, що знаходяться на даний момент в апаратній черзі. Надмірна затримка черги може привести до тремтіння трафіку - явища, дуже негативного в контексті передачі інформації масштабу реального часу (наприклад, оцифрованої мови). Стандартний апаратний буфер інтерфейсу може вміщати від одного до п'яти пакетів. Відповідно до реалізації операційної системи, більшість інтерфейсів автоматично зменшують розмір своєї апаратної черги до 2 за умови застосування алгоритму WFQ. Мережний оператор повинен мати можливість змінювати розміри апаратних черг інтерфейсів залежно від існуючих вимог до затримки трафіку. Це твердження особливе справедливо для трафіку масштабу реального часу, такого, як голосовий трафік. Розмір апаратної черги інтерфейсу може бути змінений за допомогою спеціальної команди.

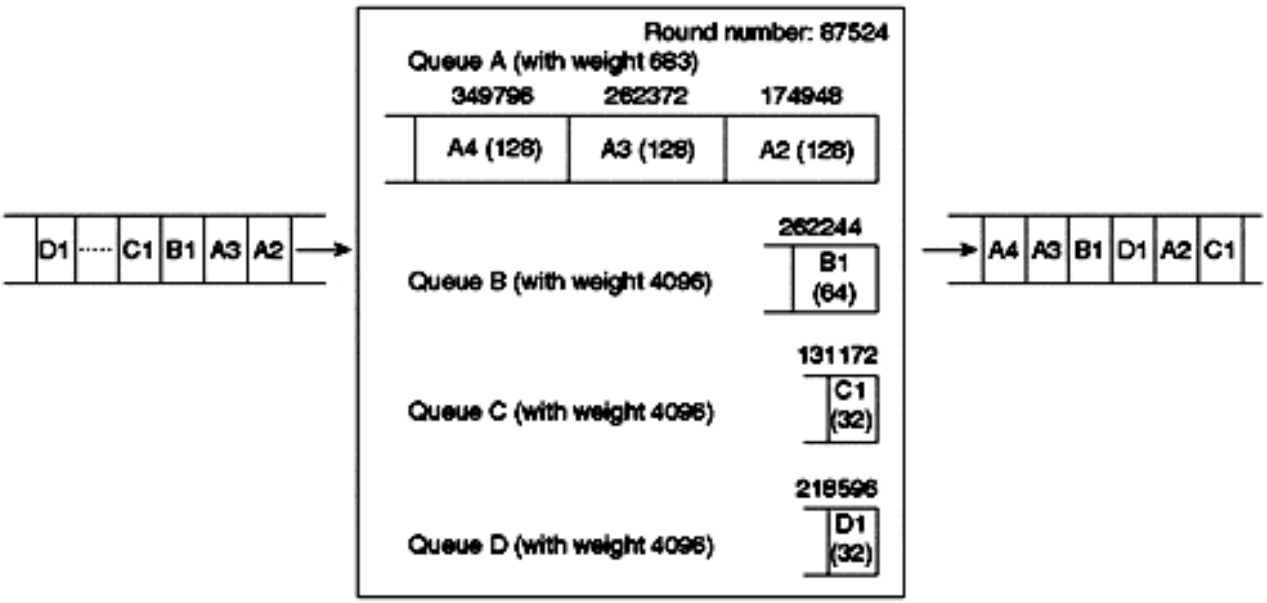


Рис. 6.21. Зміна в порядку обслуговування пакетів, викликане вступом пакетів D1 і A4

Зважений механізм рівномірного обслуговування черг (WFQ) на основі потоку використовує для обробки кожного потоку трафіку так звану підчергу. Черги механізму WFQ на основі потоку називаються також чергами діалогу (conversation queue). Оскільки пам'ять є кінцевим ресурсом, число черг діалогу за умовчанням обмежене 256. Збільшення кількості черг призводить до збільшення пам'яті, потрібної для розміщення структур даних черг, а також до збільшення об'єму підтримуваної маршрутизатором інформації про стан системи. Якщо число потоків перевищить число черг, допускається використання однієї черги для обробки декількох потоків. Слід зазначити, що збільшення числа черг природним чином зменшує шанси подібного розвитку ситуації (кожному потоку відповідає своя власна черга).

Мережний адміністратор конфігурує зважений механізм рівномірного обслуговування черг (WFQ) на основі потоку, відповідно до якого:

- активні потоки трафіку з однаковим IP-пріоритетом отримують рівні долі смуги пропускання інтерфейсу;
- активні потоки з великим IP-пріоритетом отримують велику частку смуги пропускання інтерфейсу, ніж активні потоки з меншим IP-пріоритетом.

Розглянемо приклад розподілу смуги пропускання залежно від ваги потоку.

Дано: на послідовному інтерфейсі з конфігурованим зваженим алгоритмом рівномірного обслуговування черг на основі потоку обробляється 8 потоків трафіку – поодинці на кожне значення IP-пріоритету.

Визначити:

1) Як розподіляється смуга пропускання для кожного потоку ?

2) Як зміниться розподіл смуги пропускання для кожного потоку, якщо на послідовному інтерфейсі оброблятимуться 25 потоків трафіку - 18 потоків з IP-пріоритетом 1 і по одному потоку на кожне значення IP-пріоритету, що залишилося?

Ширина смуги пропускання, яка виділена потоку трафіку, обернено пропорційна його вазі. Відповідно до зваженого алгоритму рівномірного обслуговування черг (WFQ) на основі потоку вага потоку розраховується по наступній формулі:

$$Вес = \frac{4096}{IP\ пріоритет + 1}$$

Отже, ширина смуги пропускання, виділеної для потоку трафіку, прямо пропорційна величині (IP-пріоритет + 1).

Кожному потоку трафіку виділяється частина доступної смуги пропускання каналу пропорційно величині (P+1), де P – це IP-пріоритет пакетів потоку. Кіневе значення виділеної потоку смуги пропускання

залежить від інших потоків, що розділяють між собою даний канал передачі інформації.

У першому випадку ми маємо справу з 8 потоками – по одиниці на кожне значення IP-пріоритету.

Потік трафіку з IP-пріоритетом 0 отримує:

$$\frac{1}{1+2+3+4+5+6+7+8} = \frac{1}{36} \text{ смуги пропускання каналу}$$

Потік трафіку з IP-пріоритетом 1:

$$\frac{2}{1+2+3+4+5+6+7+8} = \frac{2}{36} \text{ смуги пропускання каналу}$$

Потік трафіку з IP-приоритетом 2 – отримає 3/36 смуги пропускання каналу і так далі. Потік трафіку з IP-приоритетом 7 отримає 8/36 смуг пропускання каналу.

У другому випадку число потоків зростає до 25 - 18 потоків з IP-пріоритетом 1 і по одному потоку на кожне значення IP- пріоритету, що залишилося.

Тепер кожен потік трафіку з IP-пріоритетом 0 отримує всього лише

$$\frac{1}{1+(2*18)+3+4+5+6+7+8} = \frac{1}{70} \text{ смуги пропускання каналу}$$

Кожен потік трафіку з IP-приоритетом 1:

$$\frac{2}{1+(2*18)+3+4+5+6+7+8} = \frac{2}{70} \text{ смуги пропускання каналу і так далі}$$

Потік трафіку з IP-приоритетом 7 отримає 8/70 смуг пропускання каналу.

6.3.6.6 Зважений алгоритм рівномірного обслуговування черг) на основі класу (CBWFQ)

Відповідно до алгоритму зваженого рівномірного обслуговування черг на основі класу (Class-Based WFQ - CBWFQ) підчерга виділяється для обробки класу трафіку, а не його окремого потоку, як передбачається алгоритмом WFQ на основі потоку. Таким чином, алгоритм CBWFQ може бути отриманий шляхом доопрацювання існуючих реалізацій алгоритму WFQ на основі потоку. Для цього до алгоритму WFQ на основі потоку необхідно додати модуль класифікації трафіку, відповідно до якого підчерга WFQ буде призначена для обслуговування класу трафіку, а не його окремого потоку. Отже, реалізація алгоритму CBWFQ заснована на обчисленні порядкових номерів пакетів. Цей алгоритм підтримує всі класи, включені в цей набір. Клас трафіку може бути визначений на основі різних параметрів, таких, як IP- пріоритет, код DSCP (Differentiated Serviced Code Point – код диференційованої послуги), вхідний інтерфейс і QoS-група.

Алгоритм CBWFQ дозволяє явно вказати необхідну мінімальну смугу пропускання для кожного класу трафіку. Це вигідно відрізняє даний алгоритм від алгоритму WFQ на основі потоку, відповідно до якого мінімальна смуга пропускання потоку визначалася неявно на підставі вагів всіх активних потоків WFQ-системи.

6.3.6.7 Механізм CBWFQ з пріоритетною чергою

Для того, щоб бути зрозумілим для слухача, голосовий трафік повинен випробовувати при передачі мінімальну затримку і тремтіння (варіацію затримки). Не дивлячись на те що механізм CBWFQ може забезпечити необхідну смугу пропускання, він не в змозі гарантувати прийнятного для голосового трафіку діапазону тремтіння. Голосовий трафік характеризується порівняно невеликими запитами до смуги пропускання (як правило, 64 Кбіт/с), проте набагато жорсткішими вимогами до рівня затримки і тремтіння. З метою мінімізації затримки і тремтіння голосового трафіку механізм CBWFQ модифікуються шляхом додавання однієї або декількох черг із строгим пріоритетом. Черга із строгим пріоритетом називається також чергою з малою затримкою (low latency queue).

Окрім голосового трафіку, черги із строгим пріоритетом можуть використовуватися для обробки трафіку будь-яких застосувань, що функціонують в масштабі реального часу і чутливих до затримки пакетів.

Механізм CBWFQ з пріоритетною чергою дозволяє забезпечити обслуговування чутливого до затримок трафіку (наприклад, голосового) за допомогою використання черги із строгим пріоритетом; при цьому всі останні класи трафіку обробляються за допомогою стандартного планувальника CBWFQ. Механізм CBWFQ з пріоритетною чергою називається також механізмом обслуговування черг з малою затримкою (low latency queuing — LLQ).

Відповідно до вдосконаленого механізму CBWFQ голосовий трафік обробляється за допомогою однієї пріоритетної черги, яка по своїх характеристиках нагадує високопріоритетну чергу механізму пріоритетного обслуговування. Черги, що залишилися, є стандартними чергами механізму CBWFQ (по одній черзі на клас трафіку), що забезпечують диференціацію різних класів трафіку і гарантований розподіл пропускної спроможності інтерфейсу на основі ваги або явної вказівки смуги пропускання черги.

Голосовий трафік може бути ідентифікований на основі номерів портів транспортного протоколу масштабу реального часу (Real-time Transport Protocol – RTP). Аби призначити для обробки голосового трафіку пріоритетну чергу, слід застосувати команду "ip rtp priority" на відповідному вихідному інтерфейсі маршрутизатора.

Завантаженість пріоритетної черги може привести до “пригнічення” нею черг інтерфейсу, що залишилися, знижуючи ефективність обслуговування стандартних класів трафіку механізму CBWFQ до менш ніж задовільною. З метою зменшення цієї проблеми мережний адміністратор може задати максимальну смугу пропускання для трафіку, що обслуговується за допомогою пріоритетної черги. Якщо інтенсивність трафіку перевищить максимальне значення, весь надлишковий трафік буде відкинутий. Слід зазначити, що подібний спосіб обмеження трафіку є вельми грубим, бо він враховує лише виділену для пріоритетної черги смугу пропускання, не звертає уваги при цьому на сам голосовий виклик.

Сума смуг пропускання пріоритетної і стандартних черг механізму CBWFQ не повинна перевищувати 75 відсотків обший смуги пропускання інтерфейсу. Подібне рішення було прийняте з метою надання смуги пропускання для некласифікованого трафіку і інкапсульованої інформації рівня 2 еталонних моделі OSI

Навіть не дивлячись на наявність пріоритетної черги, механізм CBWFQ не може гарантувати негайну передачу пакетів голосового трафіку. Це пов'язано з тим, що у момент надходження голосового пакету планувальник CBWFQ, мабуть, вже обробляє який-небудь пакет даних і йому необхідно повністю завершити його передачу по лінії зв'язку. Пакети голосового трафіку мають невеликий розмір, проте розмір оброблюваних в CBWFQ - чергах пакетів може виявитися значним, а від нього прямо пропорційно залежить величина потенційної затримки пакетів голосового трафіку.

Найбільш відчутно затримка голосових пакетів виявляється при їх передачі через низькошвидкісні інтерфейси маршрутизаторів. Аби зменшити затримку голосового трафіку, мережному адміністраторові може стати необхідним сконфігурувати на низькошвидкісних інтерфейсах механізм фрагментації багатоканального двоточкового протоколу (Multilink Point-to-Point – MlPP). MLPP-фрагментація дозволяє розбити великий пакет даних на декілька дрібних частин і передавати їх, чергуючи з передачею пакетів голосового трафіку.

Підсумовуючи вищенаведене, можна зробити такі висновки:

1) У моменти перевантаження мережі механізм обслуговування черг може виділити певну смугу пропускання для потоку (класу) трафіку

шляхом регулювання порядку обслуговування пакетів у відповідній цьому потоку (класу) черги.

2) Зважений механізм обслуговування черг (WFQ) на основі потоку передбачає виділення всім потокам трафіку з однаковою вагою рівних доль смуги пропускання завдяки використанню максимінного алгоритму рівномірного розподілу ресурсів.

3) Для потоків трафіку з різною вагою, саме вага і визначає смугу пропускання, що надається цим потокам. Механізм CBWFQ є зваженим механізмом обслуговування черг (WFQ) на основі класу. Відповідно до механізму CBWFQ кожен клас трафіку поміщається в окрему підчергу і обслуговується залежно від виділеної йому смуги пропускання.

4) Механізми пріоритетного обслуговування були створені на базі використання черги із строгим пріоритетом і схеми кругового обслуговування. Мінімальне тремтіння при передачі голосового трафіку може забезпечити модифікований шляхом додавання черги із строгим пріоритетом механізм CBWFQ .

6.3.6.8 Модифікований алгоритм зваженого кругового обслуговування (MWRR)

Найбільш відповідний алгоритм обслуговування черг для заданого маршрутизатора залежить від використовуваної в ньому (маршрутизаторі) архітектури комутації пакетів.

Наприклад, зважений алгоритм рівномірного обслуговування черг (Weighted Fair Queuing - WFQ) є ідеальним вибором для маршрутизаторів Cisco, побудованих на базі шинної архітектури. У маршрутизаторах Cisco, що використовують для комутації пакетів спеціалізовану комутаційну матрицю, застосовуються інші алгоритм обслуговування черг, наприклад, модифікований алгоритм зваженого кругового обслуговування (Modified Weighted Round Robin - MWRR), або модифікований алгоритм кругового обслуговування з дефіцитом (Modified Deficit Round Robin - MDRR). Алгоритми MWRR і MDRR мають багато схожості з алгоритмом WFQ, оскільки вони теж моделюють узагальнену схему розділення процесорного часу (Generalized Processor Sharing – GPS).

Механізм кругового обслуговування, який оброблює за цикл один пакет (замість нескінченно малого об'єму даних) з кожної непорожньої черги, є найпростішою реалізацією схеми GPS. Найбільш точна імітація планувальника GPS досягається в разі рівності розміру всіх пакетів. Зважений алгоритм кругового обслуговування (Weighted Round Robin —

WRR) є розширенням планувальника кругового обслуговування, відповідно до якого кожному потоку трафіку призначається своя вага. Алгоритм WRR обробляє потік трафіку пропорційно його вазі.

Найбільш оптимальним чином WRR-планувальник узгоджується з механізмом комутації ATM (Asynchronous Transfer Mode – режим асинхронної передачі), у відповідності яким пакет представляється у вигляді чарунок, а алгоритм WRR використовується для обробки черг, що складаються з чарунок. По суті, WRR є механізмом кругового обслуговування на основі чарунок, в якому вага потоку визначає число чарунок, що обслуговуються за один цикл. Отже, кожній черзі виділяється частина смуги пропускання інтерфейсу відповідно до ваги потоку трафіку, не залежна від розміру пакету.

При необхідності замість обслуговування чарунок алгоритм WRR може використовуватися для обслуговування пакетів. В цьому випадку за один цикл планувальник WRR повинен буде обробити всі чарунки пакету. З метою підтримки пакетів змінного розміру модифікований зважений алгоритм кругового обслуговування (MWRR) використовує лічильник дефіциту, що асоціюється з кожною WRR-чергою. Це додає алгоритму MWRR деякі властивості алгоритму кругового обслуговування з дефіцитом (Deficit Round Robin - DRR), детальніший опис якого наводиться в наступному розділі цієї глави.

Алгоритм MWRR базується на наступних ключових положеннях:

1) Кожній черзі привласнюється певна вага.

2) Для кожної черги існує відповідний їй лічильник дефіциту. Причому перед початком обслуговування черг значення цього лічильника встановлюється рівним вазі черги. Лічильники вводяться для того, щоб підтримати обробку пакетів змінного розміру.

3) Обробка пакету здійснюється лише в тому випадку, якщо значення лічильника дефіциту більше нуля.

4) Після обслуговування пакету, що складається з n чарунок, значення лічильника дефіциту зменшується на n, тобто після обслуговування пакету значення лічильника дефіциту зменшується на кількість чарунок, з яких складається цей пакет.

5) Обробка пакетів проводиться до тих пір, поки значення лічильника дефіциту залишається більше нуля. Потім планувальник переходить до обслуговування наступної черги.

6) У кожному новому циклі значення лічильника дефіциту черги збільшується на вагу черги. Якщо значення лічильника дефіциту все ще менше нуля або дорівнює нулю, обробка пакету не проводиться.

Використання лічильника дефіциту дозволяє алгоритму MWRR легко справлятися з обробкою пакетів змінного розміру.

Ефективна ширина смуги пропускання черги прямо пропорційна її вазі і розраховується по наступній формулі:

$$\textit{ефективна ширина смуги пропускання} = \frac{\text{вага } \textit{черги}}{\text{сума ваг всіх активних черг}} \bullet \textit{ширина смуги пропускання інтерфейса}$$

Розглянемо функціонування алгоритму MWRR на наступному прикладі. Передбачимо, що алгоритм MWRR використовується для обслуговування трьох черг, вага кожної з них приведена в таблиці 6.8.

Таблиця 6.8. Вага черг, що обслуговуються за допомогою алгоритму

Queue (черга)	Weight (вага)
2	4
1	3
0	2

Схематичне зображення черги наводиться на рис. 6.22. Кожна черга складається з дев'яти чарунок. Чарунки, з яких складається один пакет забарвлені однаково. Черга 2 складається з трьох пакетів, кожен з яких, у свою чергу, складається з двох, трьох і чотирьох чарунок відповідно (справа наліво), значення лічильника дефіциту для кожної черги до початку обслуговування наводиться в таблиці 6.9.

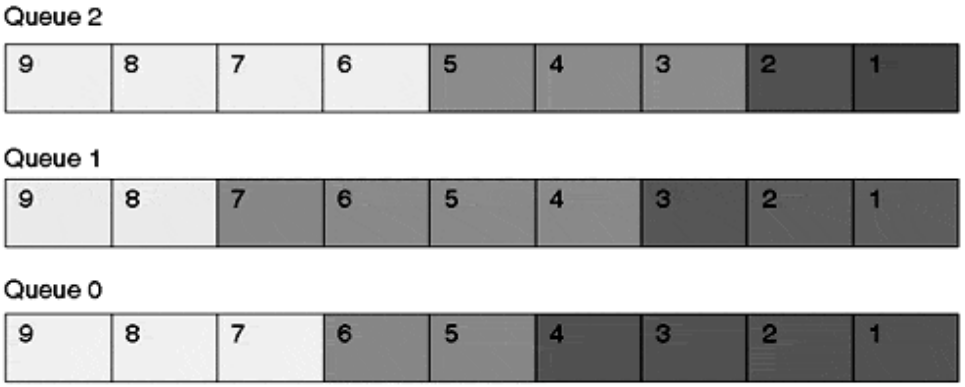


Рис. 6.22. Черги MWRR (Modified Weighted Round Robin) до початку обслуговування

Таблиця 6.9. Значення лічильника дефіциту для кожної черги до початку обслуговування

Черга	**Лічильник дефіциту**
0	2

1	3
2	4

Першою обслуговується черга 0. При ініціалізації лічильника дефіциту йому привласнюється значення 2, рівне вазі черги. На чолі черги 0 знаходиться 4-чарунковий пакет. Отже, після обслуговування цього пакету значення лічильника дефіциту стане рівним 2 - 4 = -2.

Оскільки значення лічильника дефіциту негативне, черга 0 не може бути обслужена до тих пір, поки значення лічильника дефіциту не стане більше нуля (рис. 6.23, табл. 6.10).

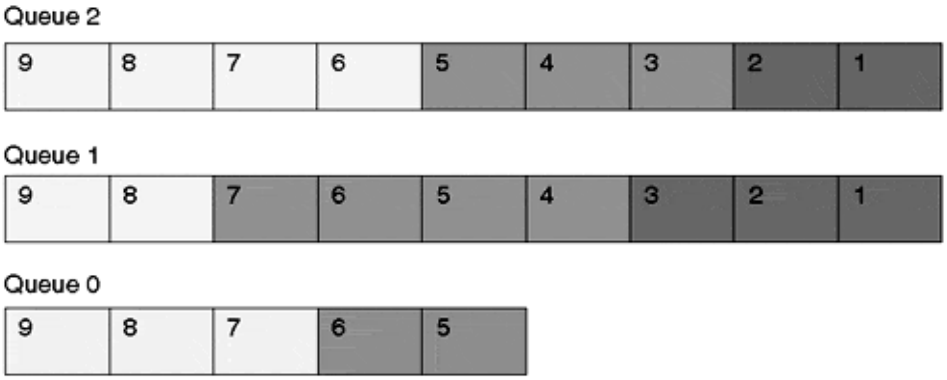


Рис. 6.23. Стан черг MWRR після першого циклу обслуговування черги 0

Таблиця 6.10. Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 0

Черга	**Лічильник дефіциту**
0	-2
1	3
2	4

Наступною обслуговується черга 1. При ініціалізації лічильника дефіциту йому привласнюється значення 3. В результаті обслуговування трьохчарункового пакету, який знаходиться на чолі черги 1, значення лічильника дефіциту стає рівним 3-3=0. Оскільки значення лічильника дефіциту дорівнює нулю, планувальник алгоритму MWRR приступає до обробки наступної черги (рис. 6.24, табл. 6.11).

Таблиця 6.11. Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 1

Черга	**Лічильник**

	дефіциту
0	-2
1	0
2	4

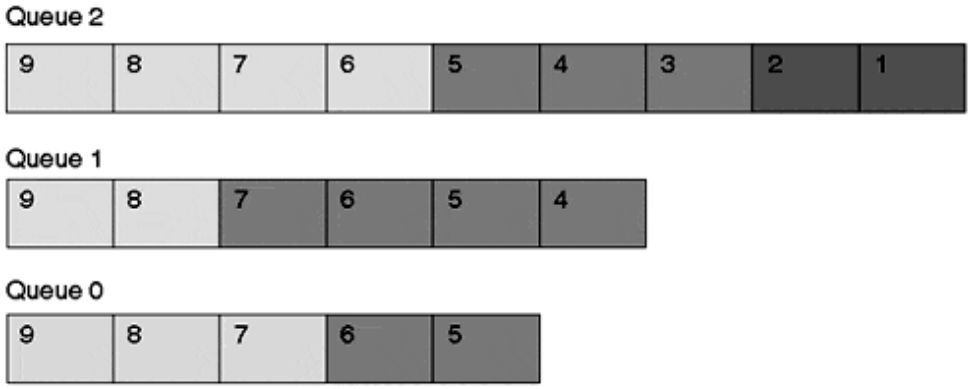


Рис. 6.24. Стан черг MWRR після першого циклу обслуговування черги 1

Останньою обслуговується черга 2. При ініціалізації лічильника дефіциту йому привласнюється значення 4. В результаті обслуговування двохчарункового пакету, який знаходиться на чолі черги 2, значення лічильника дефіциту стає рівним 4-2=2. Оскільки значення лічильника дефіциту більше нуля, MWRR-планувальник обробляє наступний, 3-чарунковий, пакет. Після обслуговування 3-чарункового пакету значення лічильника дефіциту черги 2 стає рівним 2-3 =-1, як показано на рис. 6.25.

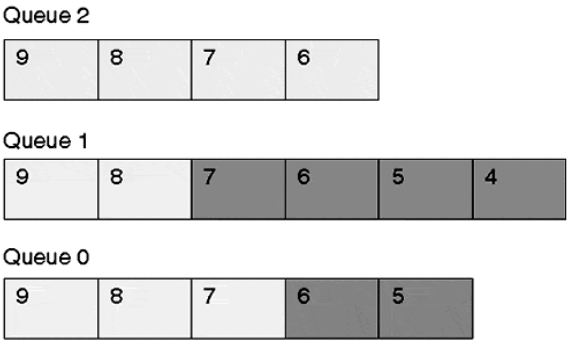


Рис. 6.25. Стан черг MWRR після першого циклу обслуговування черги 2

Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 2 наводиться в таблиці 6.12.

Таблиця 6.12. Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 2

Черга	**Лічильник дефіциту**
0	-2
1	0
2	-1

Планувальник MWRR приступає до другого циклу обслуговування черги 0. Значення лічильника дефіциту черги 0, встановлене на першому циклі, рівно -2. В результаті збільшення значення лічильника дефіциту на вагу черги воно стає рівним -2 + 2 = 0. Оскільки значення лічильника дефіциту все ще не більше нуля, планувальник алгоритму MWRR приступає до обробки наступної черги (рис. 6.26, табл.6.13).

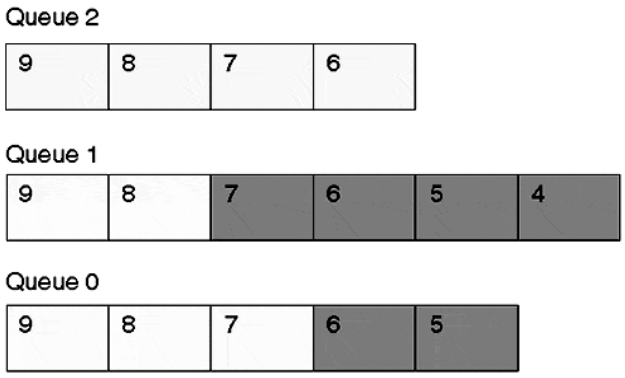


Рис. 6.26. Стан черг MWRR після другого циклу обслуговування черги 0

Таблиця 6.13. Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 0

Черга	**Лічильник дефіциту**
0	0
1	0
2	-1

Після першого циклу обслуговування значення лічильника дефіциту черги 1 дорівнювало нулю. У другому циклі обслуговування значення лічильника дефіциту збільшується на вагу черги і стає рівним 0 + 3 = 3. В результаті обслуговування вартого на чолі черги 1 четырехъячеечного пакету значення лічильника дефіциту стає рівним 3-4 =-1, як показано на рис. 6.27 і табл.6.14.

Таблиця 6.14. Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 1

Черга	Лічильник дефіциту
0	0
1	-1
2	-1

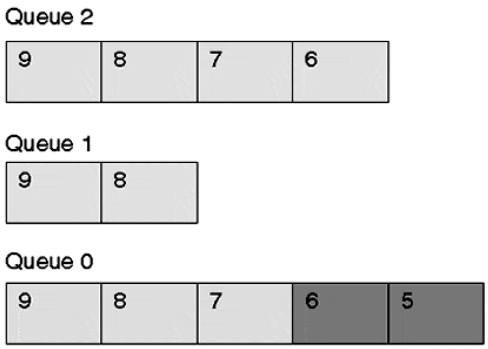


Рис.. 6.27. Стан черг MWRR після другого циклу обслуговування черги 1

У другому циклі обслуговування значення лічильника дефіциту черги 2 збільшується на її вагу і стає рівним -1+4 = 3. В результаті обслуговування чотирьохчарункового пакету, що знаходиться на чолі черги 2, значення лічильника дефіциту стає рівним 3 -4 = -1. Оскільки тепер черга 2 стає порожній, значення її лічильника дефіциту скидається в нуль (рис.6.28, табл.6.15).

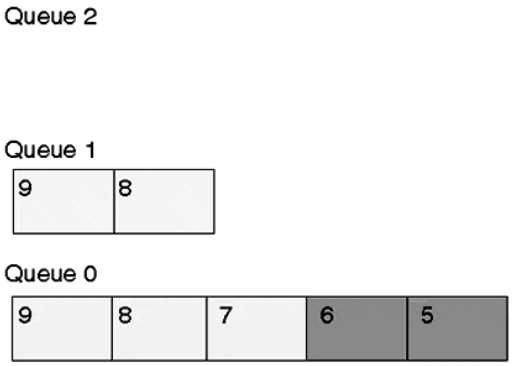


Рис.. 6.28. Стану черг MWRR після другого циклу обслуговування черги 2

Таблиця 6.15. Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 2

Черга	Лічильник дефіциту
0	0
1	-1
2	-1

Планувальник MWRR приступає до третього циклу обслуговування черги 0. Значення лічильника дефіциту збільшується і стає рівним 0 + 2 = 2. В результаті обслуговування що стоїть на чолі черги 0 двохосередкового пакету значення лічильника дефіциту стає рівним 2-2=0. MWRR - планувальник припиняє обробку черги 0 і переходить до черги 1 (рис. 6.29, табл.6.16).

Таблиця 6.16. Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 2

Черга	Лічильник дефіциту
0	0
1	-1
2	0

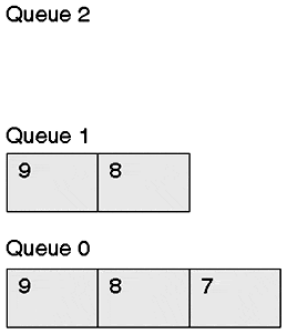


Рис. 6.29. Стан черг MWRR після третього циклу обслуговування черги 0

Нове значення лічильника дефіциту черги 1 дорівнює -1+3 = 2. У результаті обслуговування 2-чарункового пакету, що знаходиться на чолі черги 1, значення лічильника дефіциту стає рівним 2-2 = 0. Оскільки тепер черга 1 стає порожній, планувальник алгоритму MWWRR приступає до обробки черги 0, як показано на рис.6.30, табл.6.17.

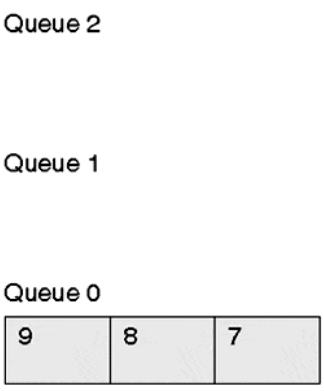


Рис. 6.30. Стан черг MWRR після третього циклу обслуговування черги 1

У четвертому циклі обслуговування черги 0 значення її лічильника дефіциту стає рівним 2. В результаті обслуговування 3-чарункового пакету, що стоїть на чолі черги 0 значення лічильника дефіциту стає рівним -1. Оскільки тепер черга 0 стає порожній, значення її лічильника дефіциту скидається в нуль.

Таблиця 6.17. Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 2

Черга	**Лічильник дефіциту**
0	0
1	0
2	0

Розглянемо деякі можливі реалізації алгоритму MWRR.

Конкретні реалізації алгоритму MWRR в тому або іншому пристрої розрізняються між собою в термінах кількості доступних MWRR-черг і способу класифікації трафіку. Наприклад, реалізація алгоритму MWRR в деяких маршрутизаторах Cisco передбачає наявність чотирьох черг на два будь-яких інтерфейсі маршрутизатора; класифікація трафіку при цьому проводиться на основі значення групи бітів поля типа обслуговування (Type of Service - ToS). Розподіл трафіку по класах ToS представлений в табл.6.18.

Таблиця. 6.18. Розподіл трафіку по класах ToS для алгоритму MWRR.

Біти поля IP - пріоритету	Біти класу ToS	Клас ToS
000	00	0
001	00	0
010	01	1
011	01	1
100	10	2
101	10	2
110	11	3
111	11	3

Ще одна реалізація алгоритму MWRR в комутаторах Cisco передбачає наявність двох черг - черги 1 і черги 2. Класифікація трафіку проводиться на 2-м рівні еталонної моделі OSI на підставі значення поля класу обслуговування (Class of Service - CoS), визначеного в специфікації IEEE (Institute of Electrical and Electronics Engineers) 802.1p. Фрейми із значенням поля CoS 0-3 ставляться в чергу 1, а фрейми із значенням поля CoS 4-7 – в чергу 2.

Приклад: алгоритм MWRR на основі класу трафіку

Постачальник послуг Internet прийняв рішення розділити магістральний трафік на 4 класи залежно від значення поля IP-пріоритету (табл. 6.19). Кожному класу відповідають два значення IP-приоритета – поодинці для погодженого і надлишкового трафіку. Трафіку класів 0-3 необхідно виділити 15, 15, 30 і 40 відсотків смуги пропускання каналу зв'язку, відповідно. Стандартний розподіл ваги для класів ToS 0-3 складає 1, 2, 4 і 8, відповідно. Отже, класам ToS 0-3 буде виділено 1/15, 2/15, 4/15 і 8/15 частин ефективної смуги пропускання інтерфейсу.

Таблиця. 6.19. Класифікація трафіку на підставі IP-приоритета

Тип трафіку	Критичний (клас 3)	Елітний (клас 2)	Стандартний (клас 1)	Економічний (клас 0)
Погоджений трафік	Пріорітет7	Пріоритет 5	Пріоритет 3	Пріоритет 1
Надлишковий трафік	Пріоритет 6	Пріоритет 4	Пріоритет 2	Пріоритет 0

У даному випадку розподіл смуги пропускання для класів 0-3 складає 15:15:30:40 або 3:3:6:8, оскільки алгоритм WRR допускає використання ваги лише в діапазоні від 1 до 15.

6.3.6.9 Модифікований алгоритм кругового обслуговування з дефіцитом (MDRR)

Модифікований алгоритм кругового обслуговування з дефіцитом (Modified Deficit Round Robin - MDRR) використовується для розподілу ресурсів в маршрутизаторах.

Алгоритм кругового обслуговування з дефіцитом (DRR) функціонує (DRR- планувальник) таким чином:

1) Кожна черга характеризується пов'язаним з нею квантовим значенням (quantum value) – середнім числом байтів, що обслуговуються на кожному циклі, – і лічильником дефіциту, початкове значення якого встановлюється рівним квантовому значенню. Квантове значення прийнято вибирати рівним розміру в байтах пакету максимального об'єму (MTU - Maximum Transmission Unit).

2) Кожна непорожня черга обробляється за круговим принципом. Сума розмірів обслуговуваних за один цикл пакетів приблизно дорівнює квантовому значенню черги.

3) Обробка пакетів черги проводиться до тих пір, поки значення лічильника дефіциту залишається більше нуля.

4) В результаті обслуговування кожного пакету значення лічильника дефіциту черги зменшується на величину, рівну розміру пакету в байтах. Тобто, об'єм даних, які будуть оброблені в наступному циклі обслуговування черги, розраховується як різниця квантового значення і лічильника дефіциту. Коли значення лічильника дефіциту стає менше нуля або рівним нулю, DRR-планувальник переходить до обробки наступної черги.

5) У кожному новому циклі значення лічильника дефіциту збільшується на величину, рівну квантовому значенню.

Механізм MDRR є модифікованим узагальненим алгоритмом DRR шляхом додавання так званої черги з малою затримкою (low-latency queue). Відповідно до алгоритму MDRR всі черги, за винятком черги з малою затримкою, обслуговуються за круговим принципом. Черга з малою затримкою може обслуговуватися в двох режимах: режимі строгого пріоритету і режимі чергуючогося пріоритету.

У режимі строгого пріоритету (strict priority mode) черга з малою затримкою обслуговується за наявності в ній хоч би одного пакету, що обумовлює мінімально можливу затримку для трафіку, який обробляється за допомогою цієї черги класу. В той же час слід зазначити, що високопріоритетна черга з малою затримкою здатна на тривалий період часу зайняти 100 відсотків смуги пропускання інтерфейсу і тим самим “подавити” MDRR-черги, що залишилися.

У режимі чергуючогося пріоритету (alternate priority mode) черга з малою затримкою обробляється в проміжках між обробкою черг, що залишилися. На додаток до черги з малою затримкою алгоритм MDRR підтримує ще сім черг. Припустимо, що черга з малою затримкою має номер 0. Тоді відповідно до режиму чергуючогося пріоритету черги механізму MDRR обслуговуються в наступному порядку: 0, 1,0, 2, 0, 3, 0, 4, 0, 5, 0, 6, 0, 7. Режим чергуючогося пріоритету дозволяє понизити максимальну затримку обслуговування черги 0 з суми квантових значень (що було б в разі традиційного механізму кругового обслуговування) до максимального квантового значення всіх черг, що залишилися.

Окрім зниження ефективності алгоритм MDRR, на відміну від алгоритму DRR, використовує нетрадиційну схему кругового обслуговування черг. Так, відповідно до алгоритму MDRR затримка обслуговування однієї вибраної користувачем черги обмежується з метою зменшення тремтіння трафіку.

Розглянемо функціонування алгоритму MDRR на наступному прикладі. Припустимо, що алгоритм MDRR використовується для обслуговування трьох черг, вага кожної з них приведена в таблиці. 6.20.

Причому, черга 2 є чергою з малою затримкою, що обслуговується в режимі пріоритету, що чергується. Квантоване значення визначається як твір MTU на вагу черги.

Таблиця 6.20. Вага черг, що обслуговуються за допомогою алгоритму

Queue (черга)	Weight (вага)	Квантоване значення=вес*MTU (MTU=1500 байт)
2	1	1500
1	2	3000
0	1	1500

Схематичне зображення черг з вказівкою відповідних ним значень лічильників дефіциту представлене на рис. 6.31и табл. 6.21.

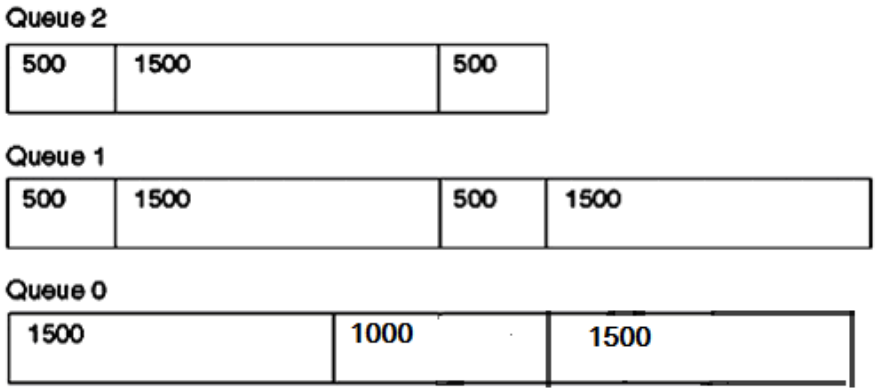


Рис. 6.31 - MDRR-черги і відповідні ним значення лічильників дефіциту до початку обслуговування

Таблиця 6.21. Значення лічильника дефіциту для кожної черги до початку обслуговування

Черга	Лічильник дефіциту
2	1500
1	3000
0	1500

Коли механізм MDRR сконфігурований на вихідному інтерфейсі маршрутизатора, в якості максимального розміру одиниці передачі інформації використовується відповідне значення MTU цього інтерфейсу.

Першою обслуговується черга 2. При ініціалізації лічильника дефіциту йому привласнюється значення 1500, рівне квантовому значенню черги. Черга 2 обслуговується до тих пір, поки відповідне їй значення лічильника дефіциту залишається більше нуля. Після обслуговування пакету значення лічильника дефіциту черги 2 зменшується на величину,

рівну розміру пакету в байтах. Оскільки поточне значення лічильника дефіциту (1500) більше нуля, планувальник MDRR обслуговує розташований на чолі черги 500-байтовий пакет. Нове значення лічильника дефіциту черги 2 стає рівним:

1500-500=1000.

Оскільки нове значення лічильника дефіциту все ще більше нуля, планувальник MDRR приступає до обслуговування наступного пакету черги. В результаті передачі 1500-байтового пакету значення лічильника дефіциту зменшується до

1000 - 1500 =-500,

після чого MDRR-планувальник переходить до обслуговування наступної черги. Стан черг і відповідних ним значень лічильників дефіциту після закінчення обслуговування черги 2 схематично представлено на рис. 6.32 і табл. 6.22.

Оскільки обслуговування черги 2 здійснюється в режимі чергуючогося пріоритету, MDRR-планувальник переходить до обробки іншої черги, номер якої вибирається відповідно до кругового принципу. Припустимо, що підійшла черга обслуговування черги 0.

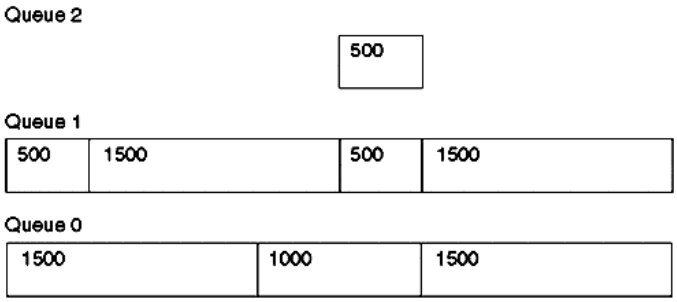


Рис. 6.32. Стан черг і відповідних ним значень лічильників дефіциту після першого циклу обслуговування черги 2

Таблиця 6.22. Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 2

Черга	Лічильник дефіциту
2	-500
1	3000
0	1500

При ініціалізації лічильника дефіциту йому привласнюється значення 1500, рівне квантовому значенню черги 0. В результаті обслуговування 1500-байтового пакету значення лічильника дефіциту зменшується до

1500 - 1500 = 0.

Відповідно до алгоритму MDRR планувальник завершує обслуговування черги 0. Стан черг і відповідних ним значень лічильників дефіциту після закінчення обслуговування черги 0 схематично представлено на рис.6.33 і табл. 6.23.

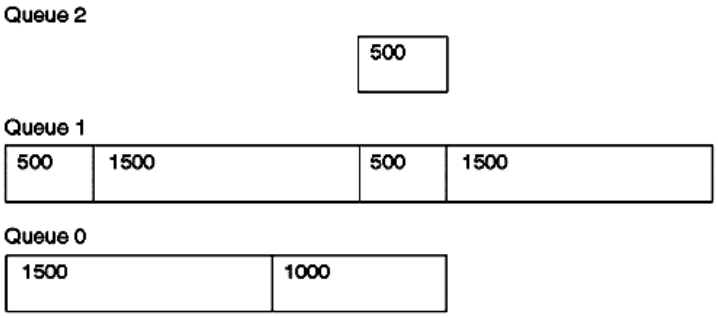


Рис. 6.33. Стан черг і відповідних ним значень лічильників дефіциту після першого циклу обслуговування черги 0

Таблиця 6.23. Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 0

Черга	Лічильник дефіциту
2	-500
1	3000
0	0

Оскільки режим чергуючогося пріоритету передбачає постійне переключення MDRR - планувальника між чергою з малою затримкою і чергами, що обробляються відповідно до кругового принципу, наступною обслуговується черга 2. Нове значення лічильника дефіциту стає рівним

-500 + 1500 = 1000.

Оскільки значення лічильника дефіциту більше нуля, MDRR - планувальник приступає до обслуговування наступного пакету черги 2. В результаті передачі 500-байтового пакету значення лічильника дефіциту зменшується до 500. Не дивлячись на те що MDRR - планувальник міг би обслужити як мінімум ще один пакет черги 2, це не представляється можливим, оскільки черга порожня. Тому значення лічильника дефіциту черги 2 встановлюється рівним нулю. Оскільки порожня черга не обробляється MDRR-планувальником, значення лічильника дефіциту черги 2 залишається рівним нулю до постановки в цю чергу наступного пакету. Стан черг і відповідних ним значень лічильників дефіциту після закінчення обслуговування черги 2 схематично представлено на рис.6.3 4 і табл. 6.24.

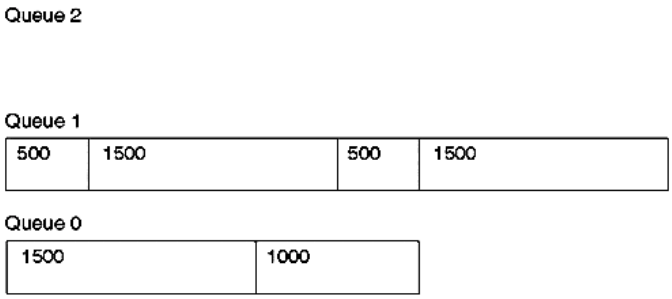


Рис. 6.34. Стан черг і відповідних ним значень лічильників дефіциту після другого циклу обслуговування черги 2

Таблиця 6.24. Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 2

Черга	Лічильник дефіциту
2	0
1	3000
0	0

Наступною обслуговується черга 1, значення лічильника дефіциту якої встановлюється рівним 3000. MDRR-планувальник передає три пакети черги 1, внаслідок чого значення її лічильника дефіциту зменшується до

3000 - 1500- 500 - 1500 = -500.

Стан черг і відповідних ним значень лічильників дефіциту після закінчення обслуговування черги 1 схематично представлено на рис. 6.35 і табл. 6.25.

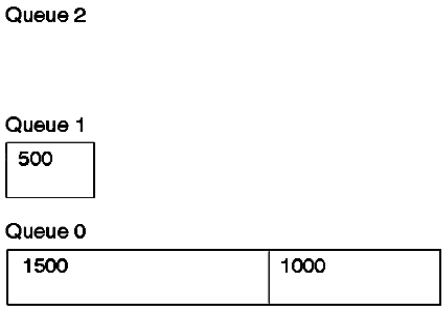


Рис. 6.35. Стан черг і відповідних ним значень лічильників дефіциту після першого циклу обслуговування черги 1

Таблиця 6.25 Значення лічильника дефіциту для кожної черги після першого циклу обслуговування черги 1

Черга	Лічильник дефіциту
2	0
1	-500

0	0

В результаті обслуговування двох пакетів черги 0 значення її лічильника дефіциту стає рівним

1500 - 1000 - 1500 = -500.

Оскільки черга 0 стає порожній, відповідне значення лічильника дефіциту скидається в нуль. Стан черг і відповідних ним значень лічильників дефіциту після закінчення обслуговування черги 0 схематично представлено на рис. 6.36 і табл. 6.26.

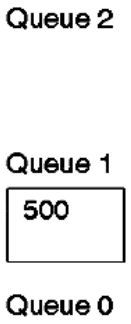


Рис. 6.36. Стан черг і відповідних ним значень лічильників дефіциту після другого циклу обслуговування черги 0

Таблиця 6.26 Значення лічильника дефіциту для кожної черги після другого циклу обслуговування черги 0.

Черга	Лічильник дефіциту
2	0
1	-500
0	0

На наступному кроці MDRR-планувальник обробляє останній пакет черги 1. Оскільки черга 1 стає порожньою, відповідне нею значення лічильника дефіциту скидається в нуль.

Підсумовуючи вищенаведене, можна зробити такі висновки:

1) Були розглянуті два нові алгоритми обслуговування черг, що використовуються для розподілу ресурсів: модифікований зважений алгоритм кругового обслуговування (Modified Weighted Round Robin - MWRR) і модифікований алгоритм кругового обслуговування з дефіцитом (Modified Deficit Round Robin - MDRR). За способом планування черг алгоритми MWRR і MDRR вельми схожі з алгоритмом WFQ.

2) При необхідності механізми MWRR і MDRR за допомогою вживання черги із строгим пріоритетом можуть бути сконфігуровані для обробки голосового трафіку.

6.3.7 PHB-політика розподілу ресурсів-запобігання перевантаження і політика відкидання

Політика відкидання пакетів (packet drop policy) є алгоритмом управління чергою, що застосовується для регулювання її довжини. Традиційний алгоритм обслуговування черг "першим прийшов, першим обслужений" (FIFO) використовує досить просту політику “відкидання хвоста” (tail drop policy), відповідно до якої будь-яка спроба постановки пакету в повну чергу неминуче завершиться його відкиданням.

Зараз основним транспортним протоколом Internet є протокол управління передачею (Transmission Control Protocol – TCP).

У цьому розділі розглядаються:

1) Механізми запобігання перевантаженню протоколу TCP, а також реакція TCP-трафіка на застосування політики “відкидання хвоста”.

2) Алгоритм довільного раннього виявлення RED (Random Early Detection), який є алгоритмом активного управління чергою, що дозволяє запобігти перевантаженню мережі шляхом превентивного відкидання пакетів з метою повідомлення про можливе перевантаження джерел TCP-з'єднання за допомогою механізму наскрізного адаптивного управління із зворотним зв'язком.

3) Зважений алгоритм довільного раннього виявлення (Weighted Random Early Detection - WRED), що дозволяє настроювати різні RED-параметри залежно від значення поля IP-пріоритету або класу трафіку. Алгоритм WRED на основі потоку (flow WRED). Цей алгоритм є розширенням алгоритму WRED, що передбачає можливість призначення штрафу з ненульовою імовірністю тим потокам, які намагаються оволодіти дуже великою часткою доступних ресурсів.

4) Алгоритм явного повідомлення про перевантаження (Explicit Congestion Notification ECN) дозволяє попередити TCP-джерело про перевантаження мережі, що починається, шляхом маркіровки (а не відкидання) пакетів.

5) Алгоритм вибіркового відкидання пакетів (Selective Packet Discard - SPD), який застосовується для управління чергою IP-процесу маршрутизатора.

6.3.7.1 Механізм повільного старту і запобігання перевантаженню

Для підтримки механізму запобігання заторам в мережі джерела TCP- з'єднання використовують так зване вікно перевантаження (congestion window - Cwnd). Ініціалізація вікна перевантаження

здійснюється у момент встановлення TCP-сеансу. Відповідно до механізму повільного старту початкове значення вікна перевантаження встановлюється рівним одному сегменту (максимальний розмір сегменту (maximum segment size - MSS) або повідомляється джерелом на іншому кінці TCP-з'єднання, або встановлюється рівним стандартному значенню і, як правило, складає 536 або 512 байт). Значення вікна перевантаження є максимальним розміром даних, які може переслати TCP-відправник в рамках заданого сеансу без отримання підтвердження про доставку.

При отриманні підтвердження про доставку першого пакету TCP-відправник збільшує розмір вікна перевантаження до 2, що вказує на можливість відправки вже двох пакетів. Аналогічно, при отриманні підтвердження про доставку двох пакетів TCP-джерело збільшує розмір вікна перевантаження до 4. Таким чином, зростання розміру вікна перевантаження є експоненціальним. Слід зазначити, що насправді зростання розміру вікна перевантаження може і не бути строге експоненціальним, оскільки TCP- одержувач, як правило, не посилає підтвердження про доставку кожного пакету, а використовує так звані підтвердження із затримкою (підтвердження про отримання двох пакетів). Описана поведінка джерел TCP- з'єднання підкоряється алгоритму повільного старту, відповідно до якого TCP-джерело передає в мережу пакети з інтенсивністю, рівній інтенсивності отримання підтверджень про доставку пакетів від TCP-одержувача. Це робить протокол TCP самосинхронизуючимся (self-clocking)транспортним протоколом.

Відповідно до протоколу TCP сигналом про перевантаження мережі є втрата пакету. TCP-джерело виявляє перевантаження за відсутності підтвердження про доставку пакету протягом заданого проміжку часу, званого оціночним часовим лімітом таймера повторної передачі (retransmit timer timeout - RTT). У ситуації, що склалася, TCP-джерело скидає значення розміру вікна перевантаження до одного сегменту і перезапускає алгоритм повільного старту. Окрім цього, він також зменшує порогове значення алгоритму повільного старту (slow start threshold - Ssthresh) до величини, рівній половині розміру вікна перевантаження у момент повторної передачі пакету. Слід зазначити, що при установці TCP-сеансу значення параметра Ssthresh встановлюється рівним або розміру вікна одержувача, повідомленого TCP-джерелом на іншому кінці з'єднання, або стандартному значенню в 65535 байт.

Після досягнення часового ліміту таймера повторної передачі (RTT) відправник слідує алгоритму повільного старту до тих пір, поки розмір вікна перевантаження не досягне величини Ssthresh. Починаючи з цього моменту розмір вікна збільшується лінійно (з коефіцієнтом 1/Cwnd) у міру отримання підтверджень про доставку пакету. Уповільнення зростання

розміру вікна перевантаження викликане тим, що значення параметра Ssthresh є оцінкою доступної смуги пропускання даного з'єднання TCP. Приклад роботи алгоритму повільного старту і алгоритму запобігання перевантаженню схематично представлений на рис.6.37.

Традиційна політика обробки пакетів, які мають бути поставлені в чергу, що досягла свого максимального розміру, полягає в їх відкиданні. Подібна “дискримінація” пакетів продовжується до тих пір, поки довжина черги не зменшиться за рахунок передачі пакетів, що вже знаходяться в ній. Алгоритм управління чергою, відповідно до якого будь-яка спроба постановки пакету в повну чергу неминуче завершиться його відкиданням, отримав назву алгоритму “відкидання хвоста ” (tail drop).

Оскільки відкидання пакету є сигналом про перевантаження мережі для джерела TCP-з'єднання, механізм “відкидання хвоста” повідомляє про перевантаження мережі лише у момент фактичного переповнювання черги. В результаті відкидання пакету джерело TCP-з'єднання зменшує розмір вікна до одного сегменту і перезапускає алгоритм повільного старту, що призводить до різкого зменшення вихідного TCP-трафіка.

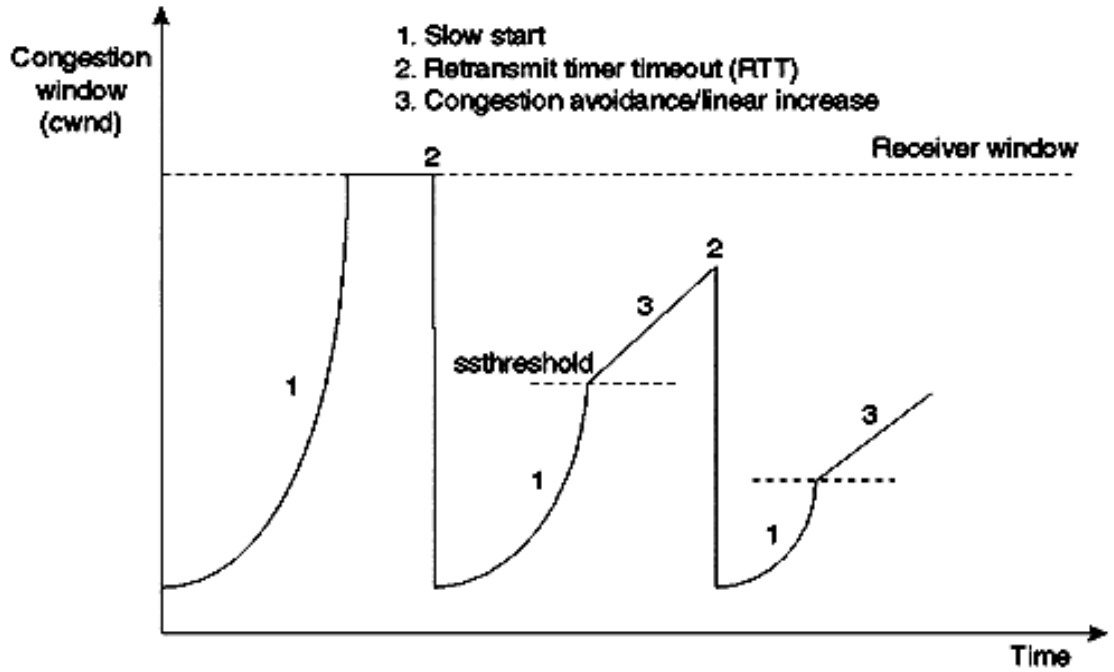


Рис. 6.37. Зміна розміру TCP - вікна відповідно до алгоритмів повільного старту і запобігання перевантаженню

Оскільки типовий магістральний маршрутизатор Internet або інший IP- мережі великого розміру в окремий момент часу обробляє тисячі TCP-потоків, застосування алгоритму управління чергою “відкидання хвоста” може привести до втрати пакетів для дуже великого числа TCP- з'єднань. Отримавши повідомлення про перевантаження мережі, множина TCP-

джерел практично одночасно зменшать інтенсивність передаваного ними трафіку, що приведе до різкого зменшення розміру черги маршрутизатора.

Всі TCP-джерела, що перезапустили механізм повільного старту і що скинули значення розміру вікна до одного сегменту, почнуть експоненціальне збільшення розмірів вікна, що веде до зростання інтенсивності оброблюваного чергою трафіку. Монотонне збільшення інтенсивності трафіку приведе до переповнювання черги і відкидання пакетів. Таким чином, алгоритм “відкидання хвоста” і удруге приведе до втрати пакетів для дуже великого числа TCP- з'єднань, а також до різкого зменшення розмірів черги. У міру збільшення розмірів TCP-вікна всіх джерел, що перезапустили механізм повільного старту, інтенсивність оброблюваного чергою трафіку зростатиме, що незабаром приведе до вже відомого сценарію розвитку подій.

Періодичне різке зниження інтенсивності трафіку і перевантаження мережі приводять до хвилеподібної зміни розміру черги, що отримала назву *ефекту глобальної синхронізації* (global synchronization). Ефект глобальної синхронізації схематично представлений на рис.6.38.

Ефект глобальної синхронізації зобов'язаний своєю назвою одночасному (синхронному) перезапуску алгоритмів повільного старту множини TCP-джерел, викликаного роботою алгоритму “відкидання хвоста”. Окрім небажаної зміни розмірів черзі, цей ефект здатний також привести до зростання тремтіння затримки трафіку і зниження пропускної спроможності всієї мережі.

Рис. 6.38. Ефект глобальної синхронізації

6.3.7.2 Алгоритм превентивного управління чергою з метою запобігання перевантаженню мережі (RED-Random Early Detection)

З поведінкою TCP-джерел в моменти роботи алгоритму “відкидання хвоста” зв'язана необхідність проведення превентивного управління чергою з метою сигналізації про перевантаження мережі до фактичного переповнювання черги і контролю за розміром черги для зниження затримки обробки пакетів. Алгоритм довільного раннього виявлення (RED) володіє істотними перевагами в порівнянні з традиційним механізмом “відкидання хвоста”.

Механізм RED використовує превентивний підхід до запобігання перевантаженню мережі. Замість чекання фактичного переповнювання черги, RED починає відкидати пакети з ненульовою імовірністю, коли середній розмір черги перевищить певне мінімальне порогове значення. Імовірнісний підхід до відкидання пакетів дозволяє бути упевненим в тому, що механізм RED відкине пакети всього лише декількох довільно вибраних потоків, тим самим допомагаючи уникнути ефекту глобальної синхронізації. Нагадаємо, що відкидання пакету є сигналом TCP-джерелу про необхідність зменшити інтенсивність передаваного трафіку для відповідного потоку, що досягається за рахунок перезапуску алгоритму повільного старту.

Якщо середній розмір черги продовжуватиме збільшуватися не дивлячись на відкидання довільних пакетів, то це приведе до лінійного зростання імовірності відкидання. Відповідно до механізму RED імовірність відкидання пакетів зростає прямо пропорційно збільшенню середнього розміру черги від мінімального до максимального порогового значення. Середній розмір черги строго обмежений максимальним пороговим значенням, оскільки в цьому випадку імовірність відкидання пакетів досягає свого найбільшого значення (100 відсотків). Іншими словами, головна мета механізму довільного раннього виявлення (RED) полягає в мінімізації середнього розміру черги, а значить, і обший затримки трафіку.

Визначення імовірності відкидання пакету базується на зваженому експоненціальному значенні середнього розміру черги. Якщо середній розмір черги вельми невеликий і знаходиться нижчим за мінімальне порогове значення, механізм RED не здатний забезпечити істотної переваги в порівнянні з традиційними механізмами управління чергою. З іншого боку, при затяжному періоді перевантаження мережі поведінка механізму RED, не дивлячись на довгу чергу і високе максимальне порогове значення, аналогічно поведінки класичного механізму “відкидання хвоста”. Таким чином, основне призначення механізму RED полягає в згладжуванні часових сплесків трафіку і попередженні

тривалого перевантаження мережі за допомогою повідомлення джерел трафіку про необхідність зниження інтенсивності передачі інформації. Якщо джерела проявлять здібність до взаємодії і одночасно зменшать інтенсивність передаваного трафіку, це допоможе запобігти перевантаженню мережі.

Інакше середній розмір черги досить швидко досягне максимального порогового значення, що приведе до відкидання всіх пакетів, що поступають на вхідний інтерфейс мережного вузла.

Основні цілі механізму раннього довільного виявлення:

1) Мінімізація тремтіння затримки пакетів шляхом контролю за середнім розміром черги.

2) Запобігання ефекту глобальної синхронізації TCP-трафіка.

3) Забезпечення неупередженого обслуговування трафіку, який характеризується короткочасними сплесками.

4) Строге обмеження максимального середнього розміру черги.

Механізм довільного раннього виявлення базується на двох наступних алгоритмах:

- Алгоритм обчислення середнього розміру черги - визначає допустимий рівень сплеску трафіку в черзі.
- Алгоритм обчислення імовірності відкидання пакетів - визначає імовірність (частоту) відкидання пакетів для заданого середнього розміру черги.

Розглянемо ці алгоритми.

І Алгоритм обчислення середнього розміру черги

При визначенні імовірності відкидання пакетів механізм RED обчислює не поточний, а експоненціально зважений середній розмір черги. Поточний середній розмір черги визначається на підставі попереднього середнього і поточного дійсного розміру. Використання механізмом RED середнього розміру черги обумовлено прагненням реагувати лише на тривале перевантаження мережі і “не помічати” моментальних сплесків трафіку.

Середній розмір черги обчислюється за формулою:

$$Q_{\text{сред}} = Q'_{\text{сред}} \cdot \left(1 - \frac{1}{2^n}\right) + Q_{\text{тек}} \cdot \frac{1}{2^n},$$

де $Q'_{\text{сред}}$ - попередній середній розмір черги;

$Q_{\text{тек}}$ - поточний розмір черги;

n - експоненціальний ваговий коефіцієнт, визначуваний користувачем.

Експоненціальний ваговий коефіцієнт є ключовим параметром, який визначає відносний вклад попереднього середнього і поточного розміру черги в новий середній розмір черги. Практика показала, що найбільш прийнятним значенням експоненціального вагового коефіцієнта *n* є 9. Збільшення експоненціального вагового коефіцієнта приведе до домінування попереднього середнього розміру черги над її поточним розміром в аспекті обчислення нового середнього розміру черги. Навпаки, зменшення експоненціального вагового коефіцієнта приведе до зростання значущості поточного розміру черги при обчисленні її нового середнього розміру.

Велике значення коефіцієнта n обумовлює математичну близькість нового і попереднього середнього розміру черги, а також дозволяє механізму RED стриманіше реагувати на моментальні зміни в її поточному розмірі, що виражається в наступній поведінці.

- Значення середнього розміру черги змінюється повільно, для нього украй нехарактерні різкі скачки. Механізм RED досить стримано відноситься до часових сплесків трафіку, прагнучи вирівняти поточний розмір черги.
- Механізм RED не квапиться ініціювати процес відкидання пакетів, який, проте, може продовжуватися деякий час після зниження дійсного розміру черги нижче за мінімальне порогове значення.
- Якщо значення коефіцієнта *n* дуже велике, механізм RED може і зовсім перестати реагувати на перевантаження мережі, оскільки в цьому випадку поточний розмір черги практично не впливатиме на обчислення її середнього розміру. Пакети передаватимуться або відкидатимуться так, як якби механізм RED і зовсім не використовувався.

Маленьке значення коефіцієнта n обумовлює математичну близькість нового середнього і поточного розміру черги, що виражається в наступній поведінці механізму RED.

- Середній розмір черги змінюється дуже швидко, для нього характерна сильна залежність від флуктуацій потоку трафіку.
- Механізм RED негайно реагує на довгу чергу, проте як тільки її розмір виявляється нижчим за мінімальне порогове значення, відкидання пакетів припиняється.
- Якщо значення коефіцієнта *n* дуже мало, механізм RED починає дуже гостро реагувати на тимчасові сплески трафіку, що виражається в невиправданому відкиданні пакетів.

ІІ Алгоритм обчислення імовірності відкидання пакетів

Імовірність відкидання пакетів є функцією, залежною від середнього розміру черги, мінімального порогового значення, максимального порогового значення і знаменника граничної імовірності (mark probability denominator), що визначає частину відкиданих пакетів при досягненні середнім розміром черги максимального порогового значення. Наприклад, якщо знаменник (дільник) граничної імовірності дорівнює 10, то при досягненні середнім розміром черги максимального порогового значення механізм RED відкидатиме 1 з 10 пакетів. Нижче приведена формула, по якій розраховується імовірність відкидання пакетів.

$$P_{drop} = \left(\frac{Q_{cp} - Q_{min}}{Q_{max} - Q_{min}} \right) \cdot p',$$

де P_{drop} - імовірність відкидання пакетів;

$Q_{\text{ср}}$ - середній розмір черги;

$Q_{\min}$ - мінімальне порогове значення розміру черги;

$Q_{\max}$ - максимальне порогове значення розміру черги;

p' - знаменник (дільник) граничної імовірності.

Коли середній розмір черги перевищує мінімальне порогове значення, механізм RED починає відкидати пакети. Інтенсивність відкидання пакетів зростає прямо пропорційно зростанню середнього розміру черги до тих пір, поки він не досягне максимального порогового значення.

Коли середній розмір черги перевищує максимальне порогове значення, механізм RED відкидає всі пакети, призначені для постановки в чергу. Графік імовірності відкидання пакетів схематично представлений на рис. 6.39.

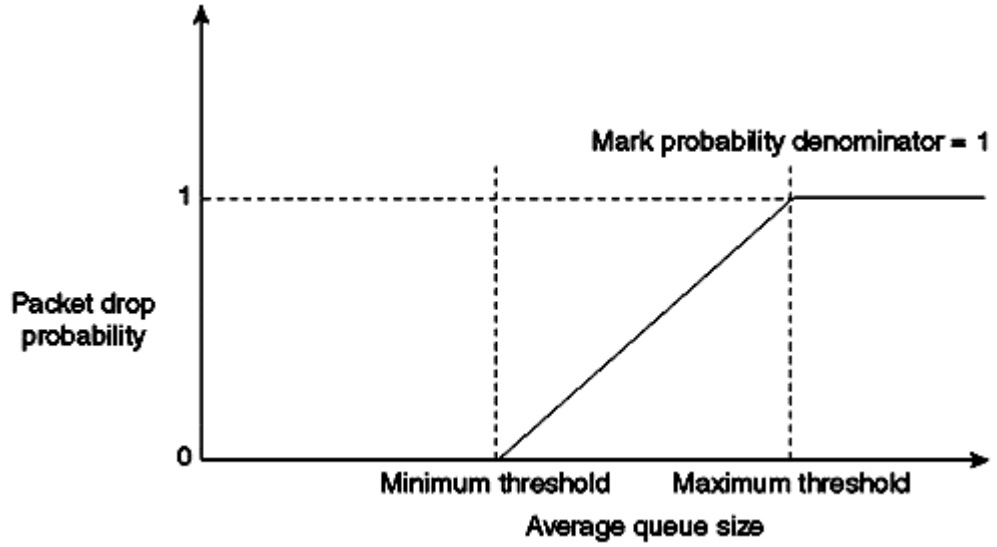


Рис. 6.39. Графік імовірності відкидання пакетів механізмом RED

6.3.7.3 Зважений алгоритм довільного раннього виявлення (WRED - Weighted Random Early Detection)

Зважений алгоритм довільного раннього виявлення (WRED) надає різні рівні обслуговування пакетів залежно від імовірності їх відкидання і забезпечує вибіркову установку параметрів механізму RED на підставі значення поля IP-пріоритета. Іншими словами, алгоритм WRED передбачає можливість інтенсивнішого відкидання пакетів, що належать певним типам трафіку, і менш інтенсивного відкидання всіх останніх пакетів.

Реалізація алгоритму зазвичай проводиться таким чином: за умовчанням всі рівні пріоритету трафіку характеризуються однаковим максимальним пороговим значенням і різними мінімальними пороговими значеннями. Таким чином механізм WRED забезпечує інтенсивніше відкидання низькопріоритетних пакетів і менш інтенсивне відкидання високопріоритетних. Стандартне мінімальне порогове значення для трафіку пріоритету 0 складає половину максимального порогового значення. Мінімальне порогове значення механізму WRED, відповідне високопріоритетному трафіку, має бути більшим, ніж мінімальне порогове значення низькопріоритетного трафіку. Виконання цієї умови необхідне для забезпечення строгої черговості відкидання пакетів, згідно якої першими починають відкидатися низькопріоритетні пакети.

Розглянемо функціонування алгоритму ***WRED на основі потоку***.

Алгоритм WRED розрахований на TCP-трафік, якій "реагує" на повідомлення про перевантаження, інакше кажучи, володіє здібністю до адаптації. Але існує ще, наприклад, UDP-трафік, який такою здатністю не володіє і не реагує на повідомлення про перевантаження і, відповідно, не знижує свою інтенсивність. Враховуючи таку поведінку UDP-трафіка, нескладно уявити собі ситуацію, в якій під час перевантаження мережі неадаптивні потоки передають дані з набагато більшою інтенсивністю, чим потоки, що володіють здібністю до адаптації. Отже, на неадаптивні потоки трафіку доводиться більша частка ресурсів в порівнянні з потоками, що знижують свою інтенсивність у відповідь на отримання сигналу про перевантаження.

Алгоритм WRED на основі потоку (flow WRED) є модифікацією алгоритму WRED, що передбачає штрафування потоків, що віднімають надмірну долю ресурсів.

З метою забезпечення рівномірного обслуговування активних потоків трафіку механізм WRED класифікує всі встановлювані в чергу пакети залежно від їх пріоритету і потоку трафіку, до якого вони відносяться. Окрім цього, WRED підтримує інформацію про стан всіх

активних потоків (active flows), тобто потоків, хоч би один пакет яких поставлений на обробку в яку-небудь з черг.

Інформація про стан активних потоків використовується для визначення справедливої долі виділених потоку ресурсів черги (розмір черги/кількість активних потоків), а також для виявлення і штрафування потоків, що віднімають надмірно великий об'єм ресурсів. Аби механізм WRED адекватніше реагував на сплески потоків трафіку, можна збільшити справедливу долю ресурсів кожного потоку шляхом застосування так званого коефіцієнта масштабування.

Справедлива доля ресурсів для активного потоку трафіку = розмір черги/кількість активних потоків.

З врахуванням коефіцієнта масштабування:

*Справедлива доля ресурсів для активному потоку трафіку = (розмір черги/кількість активних потоків)*коефіцієнт. масштабування.*

Потік, вимоги якого перевищують справедливу долю ресурсів з врахуванням коефіцієнта масштабування, штрафується шляхом збільшення ненульової імовірності відкидання для всіх пакетів, що знов надійшли.

Розглянемо дії, що робляться механізмом WRED на основі потоку у відношенні тільки що поставленого в чергу пакету.

1) При визначенні імовірності відкидання пакету механізм WRED на основі потоку враховує як значення поля IP-пріоритету пакету, так і інформацію про стан активних потоків. Від IP- пріоритету пакету залежать конфігуровані (або стандартні) мінімальне і максимальне порогові значення.

2) Якщо середній розмір черги нижчий за мінімальне порогове значення, то імовірність відкидання пакету встановлюється рівною нулю (іншими словами, цей пакет не буде відкинутий).

3) Якщо ж середній розмір черги знаходиться між мінімальним і максимальним пороговим значенням, то враховується інформація про стан активних потоків трафіку.

4) Якщо пакет належить потоку, що перевищив справедливу долю ресурсів з врахуванням коефіцієнта масштабування, механізм WRED збільшує імовірність відкидання цього пакету шляхом зменшення відповідного максимального порогового значення, як показано нижче.

Нове max порогове значення = = min поріг. значення + ((max поріг значення - min поріг. значення)/2).

Ненульова імовірність відкидання пакету розраховується на підставі мінімального і нового максимального порогового значення. Оскільки

результатом зниження максимального порогового значення є істотне збільшення кута нахилу кривої імовірності відкидання (рис. 6.40), шанси пакету бути відкинутим різко зростають.

Якщо ж потік трафіку не перевищує справедливої долі ресурсів з врахуванням коефіцієнта масштабування, то ненульова імовірність відкидання пакету розраховується по стандартному методу.

Коли середній розмір черги перевищує максимальне порогове значення, механізм WRED на основі потоку відкидає всі пакети, призначені для постановки в чергу.

Слід зазначити, що механізм WRED на основі потоку збільшує імовірність відкидання пакетів лише для тих потоків трафіку, чиї вимоги перевищили справедливу долю ресурсів з врахуванням коефіцієнта масштабування. У всьому іншому поведінка механізму WRED на основі потоку аналогічно поведінці стандартного механізму WRED.

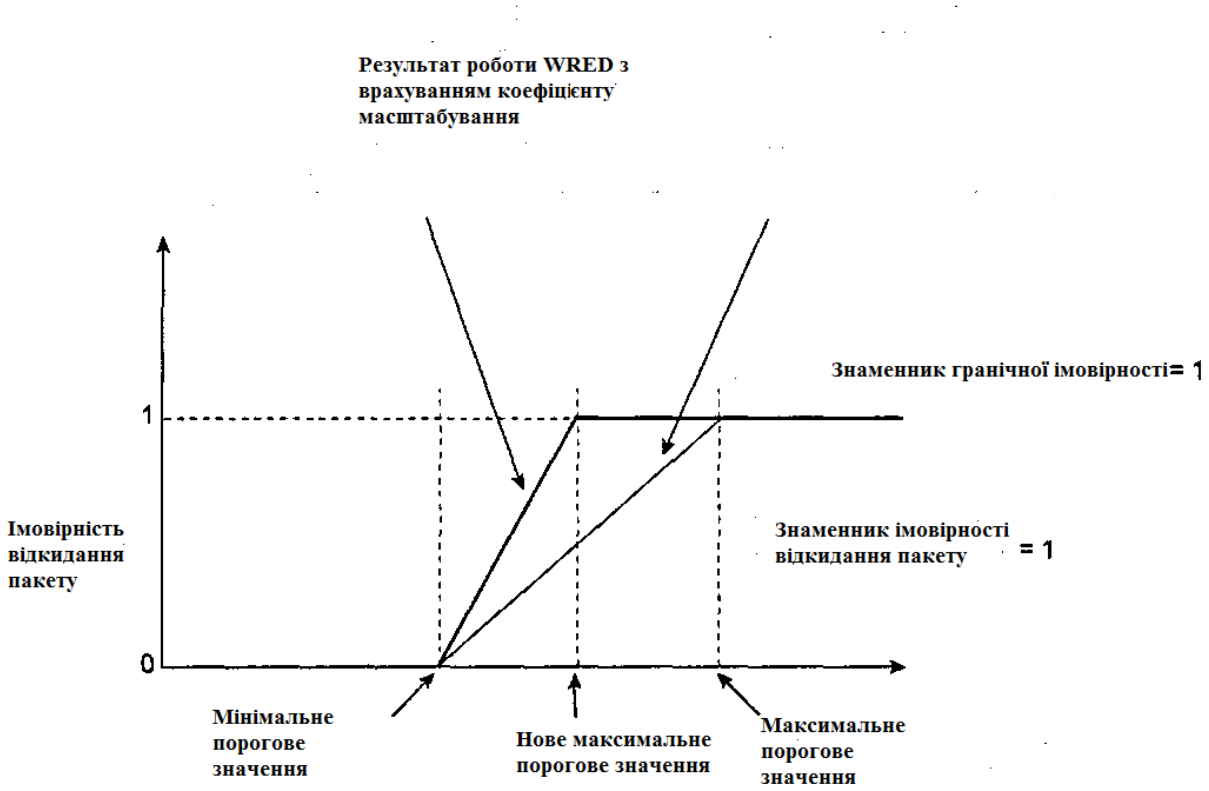


Рис. 6.40. Графік імовірності відкидання пакету при використанні механізму WRED

Механізм WRED на основі потоку встановлює ненульову імовірність відкидання пакетів при знаходженні середнього розміру черги між мінімальним і максимальним пороговими значеннями навіть для тих потоків, які характеризуються всього лише декількома поставленими в чергу пакетами. Можна конфігурувати механізм WRED на основі потоку так, щоб він не відкидав пакети подібних потоків трафіку (вказавши при

цьому, яке саме число поставлених в чергу пакетів все ще є “рятівним” для потоку) шляхом установки мінімального порогового значення, близького до максимального порогового значення. При цьому коли середній розмір черги досягне максимального порогового значення, можна застосувати механізм “відкидання хвоста”.

Контрольні запитання

1. Поясніть поняття якості обслуговування (QOS).
2. Які ви знаєте рівні QOS ?
3. Назвіть характеристики продуктивності мережного з'єднання.
4. Поясніть, що таке затримка серіализації, затримка розповсюдження і затримка комутації.
5. Поясніть, що таке джітер пакетів (packet jitter).
6. Які ви знаєте функції якості обслуговування?
7. Сформулюйте призначення протоколу резервування ресурсів RSVP.
8. Сформулюйте поняття потоку даних протоколу RSVP.
9. Назвіть типи потоків даних протоколу RSVP.
10. Визначте основні модулі протоколу RSVP і їх призначення
11. Хто є ініціатором сеансу RSVP?
12. Які ви знаєте стилі резервування по протоколу RSVP?
13. Наведіть приклад індивідуального резервування за протоколом RSVP.
14. Наведіть приклад розділеного явного резервування за протоколом RSVP.
15. Наведіть приклад розділеного неявного резервування за протоколом RSVP.
16. Узагальнена модель QoS моделі DiffServ.
17. Назвіть функції формування трафіку на границі мережі.
18. Поясніть, що таке PHB- політика.
19. Визначте поняття коду диференційованої послуги DSCP
20. Алгоритм функціонування механізму "корзина маркерів"за умови рівності погодженого і розширеного розмірів сплеску.
21. Алгоритм функціонування механізму "корзина маркерів"за умови нерівності погодженого і розширеного розмірів сплеску.
22. Поясніть сутність PHB-політики розподілу ресурсів.
23. Поясніть сутність алгоритму обслуговування черг FIFO
24. Поясніть сутність максимінної схеми рівномірного розподілу ресурсів
25. Визначить основні принципи узагальненої схеми розділення процесорного часу

26. Дано: погоджений розмір сплеску BC=5 кБайт; розширений розмір сплеску B_E =10 кБайт. Припустимо, що починаючи з деякого моменту часу поступили 3 пакети, для передачі кожного з яких займали по 1000 байт. Розрахувати значення поточного боргу DA і накопиченого боргу DC, а також імовірність відкидання пакету після передачі кожного пакету за алгоритмом "корзина маркерів".
27. Використовуючи максимінну схему рівномірного розподілу ресурсів, розподілити ресурси між користувачами A, B, З, D і E, якщо їх вимоги складають 4, 3, 3, 5 і 2 одиниць відповідно, а загальний об'єм доступного ресурсу дорівнює 13 одиницям.
28. Визначити порядок обслуговування пакетів по алгоритму WFQ на основі потоку, якщо на вхідний інтерфейс поступає три потоки трафіку, A, B і C, розміри пакетів яких складають 64, 32 і 100 байт, відповідно. Пріоритет трафіку C дорівнює 3, останніх потоків - 0. Пакети поступають один за іншим на FQ-сервер в наступному порядку: A1, C1, B1, A2, C2, B2. На момент отримання пакету A1 значення лічильника циклів дорівнює 100.
29. Написати в двійковому вигляді код DSCP для політики гарантованої передачі AF11.
30. Визначити порядок обслуговування пакетів по алгоритму WFQ на основі порядкового номера пакету, якщо на вхідний інтерфейс поступає чотири потоки трафіку, A, B, C і D розміри пакетів яких складають 128, 64 і 32, 100 байт, відповідно. Пакети поступають один за іншим на завантажений FQ-сервер в наступному порядку: A1, A2, B1, A3, C1, D1. На момент здобуття пакету A1 значення лічильника циклів дорівнює 200.
31. Поясніть сутність експоненціального вагового коефіцієнта для алгоритма WRED.
32. Що таке мінімальне та максимальне порогове значення розміру черги для алгоритма WRED?
33. Що таке ефект глобальної синхронізації і яким чином він пов'язаний з механізмом повільного старту?
34. Що таке поточний розмір черги для алгоритма WRED?
35. Наведіть аналітичний вираз для визначення середнього розміру черги за алгоритмом WRED.

Розділ 7. Рівень управління NGN.

7.1 Управління викликами в NGN. Softswitch

Рівень або площина управління викликами моделі NGN знаходиться між рівнем транспортних мереж, де зосереджені ресурси мережі і обслуговується весь трафік, і рівнем послуг. Таким чином, завдання цього рівня одночасно пов'язані з питаннями управління процесами обслуговування трафіку і надання сучасних послуг зв'язку.

Рівень управління, або, по-іншому, рівень комутації, з'явився у зв'язку з розвитком концепції виділених систем сигналізації.

Згідно визначенню Міжнародного союзу електрозв'язку ITU сигналізація – обмін інформацією (при автоматичному зв'язку), спеціально призначеною для встановлення і завершення з'єднання, а також для управління обслуговуванням викликів і мережею.

Концепція виділених систем сигналізації сходить до системи СКС №7, у якій вперше в історії розвитку систем зв'язку передбачалося розділення мовного і сигнального трафіків. Подальший розвиток цієї концепції пішов у напрямі комп'ютерної телефонії, яка передбачала не лише створення окремої виділеної мережі сигналізації, але і перетворення сигнальних повідомлень виділеними пристроями на основі комп'ютерів. Це привело до концепції Softswitch, а потім до концепції об'єднання на рівні управління мобільних і проводових мереж – концепції IMS.

Розглянемо основні компоненти рівня управління викликами, що є новою концепцією комутації, реалізованого на технології Softswitch.

7.1.1 Softswitch

Softswitch є носієм інтелектуальних можливостей мережної взаємодії, який координує управління обслуговуванням викликів, сигналізацію і функції, що забезпечують встановлення з'єднання через одну або декілька мереж.
Softswitch – це не лише один з мережних пристроїв. Це також і мережна архітектура, і навіть, певною мірою, - ідеологія побудови мережі.

Основні функції Softswitch:

- Управління обслуговуванням викликів, тобто встановленням і руйнуванням з'єднань. Дані функції гарантують, що з'єднання збережеться до тих пір, поки не дасть відбій абонент, що викликав або викликався. Також до числа функцій входять розпізнавання і обробка цифр номера, розпізнавання моменту відповіді сторони, що викликається, моменту, коли один з абонентів кладе трубку, і реєстрація цих дій для нарахування плати.

- Управління транспортними шлюзами і шлюзами доступу по протоколу H.248 і йому подібними.
- Координація обміну сигнальними повідомленнями між мережами, тобто підтримка функцій SG (Signaling Gateway). Інакше кажучи, Softswitch координує дії, що забезпечують з'єднання з логічними об'єктами в різних мережах і перетворює інформацію в повідомленнях, аби вони зрозумілі на обох сторонах несхожих мереж.

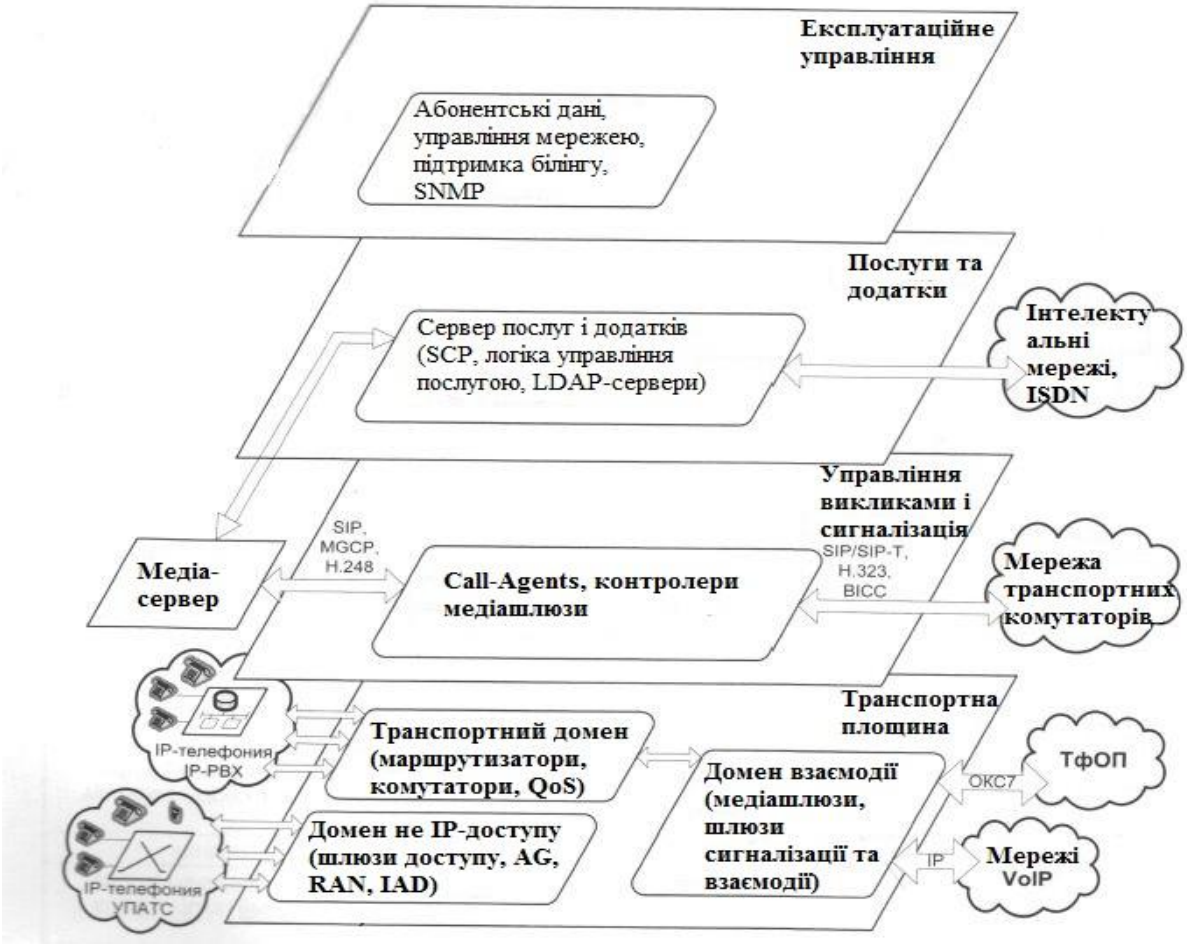


Рис. 7.1 - Еталонна архітектура Softswitch

Традиційні АТС в єдиній структурі об'єднують функції комутації, функції управління обслуговуванням викликів, послуги і застосування, а також функції білінгу. Така АТС є монолітною, закритою системною структурою, яка не допускає розширення або модернізації на базі устаткування інших виробників.

Softswitch в корені змінив традиційну закриту структуру систем комутації, використовуючи принципи компонентної побудови мережі і відкриті стандартні інтерфейси між трьома основними функціями: комутації, управління обслуговуванням викликів, послуг і застосувань. У такій відкритій, розподіленій структурі можуть застосовуватися функціональні компоненти різних виробників.

Згідно еталонній архітектурі Softswitch, розробленій консорціумом IPCC (International Packet Communication Consortium), в ній передбачається чотири представлені на рис.7.1 функціональні площини:

- транспортна;
- управління обслуговуванням виклику і сигналізації;
- послуг і застосувань;
- експлуатаційного управління.

7.1.1.1 Транспортна площина

Транспортна площина (Transport Plane) відповідає за транспортування повідомлень по мережі зв'язку. Цими повідомленнями можуть бути повідомлення сигналізації, повідомлення маршрутизації для організації тракту передачі інформації або безпосередньо призначені для користувача мова і дані. Розташований під цією площиною фізичний рівень перенесення повідомлень може базуватися на будь-якій технології, яка відповідає вимогам до пропускної спроможності для перенесення трафіку цього типа. Транспортна площина забезпечує також доступ до мережі IP-телефонії сигнальної і призначеної для користувача інформації, що поступає з боку інших мереж або терміналів. Як правило, пристроями і функціями транспортної площини управляють функції площини управління обслуговуванням виклику і сигналізації.

Сама транспортна площина ділиться на три домени:

- домен транспортування по протоколу IP;
- домен взаємодії;
- домен доступу, відмінного від IP.

Домен транспортування по протоколу IP (IP transport domain) підтримує магістральну мережу і маршрутизацію для транспортування пакетів через мережу IP-телефонії. До цього домена відносяться такі пристрої, як комутатори, маршрутизатори, а також засоби забезпечення якості обслуговування (QOS).

Домен взаємодії (Interworking Domain) включає пристрої перетворення сигнальної або призначеної для користувача інформації, що поступає з боку зовнішніх мереж, у вигляд, придатний для передачі по мережі IP-телефонії, а також зворотне перетворення. У цей домен входять такі пристрої, як шлюзи сигналізації (Signaling Gateways), що забезпечують перетворення сигнальної інформації між різними транспортними рівнями; транспортні шлюзи, або медіашлюзи (Media Gateways), що виконують функції перетворення призначеної для користувача інформації між різними транспортними мережами і різними

типами мультимедійних даних; шлюзи взаємодії (Interworking Gateways), що забезпечують взаємодію різних протоколів сигналізації на одному транспортному рівні.

Домен доступу, відмінного від IP (NON-IP Access Domain), призначений для організації доступу до мережі IP-телефонії різних несумісних терміналів. Він складається з шлюзів Access Gateways для підключення установчо-виробничих АТС, аналогових кабельних модемів, ліній xDSL, транспортних шлюзів для мобільної мережі радіодоступу стандарту GSM/3G, а також пристроїв інтегрованого абонентського доступу IAD (Integrated Access Devices) і інших пристроїв доступу. IP-термінали безпосередньо підключаються до домена транспортування по протоколу IP без участі Access Gateway.

7.1.1.2 Площина управління обслуговуванням виклику і сигналізації

Площина управління обслуговуванням виклику і сигналізації (Call Control & Signaling Plane) управляє основними елементами мережі IP-телефонії і в першу чергу тими, які належать транспортній площині. Вона управляє обслуговуванням виклику на основі сигнальних повідомлень, що поступають з транспортної площини, встановлює і руйнує з'єднання для передачі користувачевої інформації по мережі. Ця площина включає такі пристрої, як контролер медіашлюзів MGC (Media Gateways Controller), сервер обслуговування виклику Call Agent, гейткіпер Gatekeeper і LDAP-сервер (база данных плюс протокол прикладного рівня для доступу до служби каталогів X.500, розроблений IETF, що використовує TCP/IP і що дозволяє проводити операції аутентифікації (bind), пошуку (search) і порівняння (compare), а також операції додавання, зміни або видалення записів).

7.1.1.3 Площина послуг і застосувань

Площина послуг і застосувань (Service & Application Plane) містить логіку виконання послуг і застосувань в мережі IP-телефонії і управляє цими послугами шляхом взаємодії з пристроями, що знаходяться в площині управління обслуговуванням виклику і сигналізації. Площина послуг і застосувань складається з таких пристроїв, як сервери застосувань Application Servers і сервери додаткових послуг Feature Servers. Вона може також управляти спеціалізованими компонентами передачі інформації користувача, наприклад, медіасерверами, які виконують функції конференц-зв'язку, IVR (система заздалегідь записаних голосових повідомлень, що виконує функцію маршрутизації дзвінків усередині call-центра) і тому подібне.

7.1.1.4 Площина експлуатаційного управління

Площина експлуатаційного управління (Management Plane) забезпечує функції вмикання/вимикання абонентів і послуг, експлуатаційної підтримки, білінга і інші функції технічної експлуатації мережі. Площина експлуатаційного управління може взаємодіяти з деякими або зі всіма іншими трьома площинами або по стандартному протоколу (наприклад по протоколу SNMP), або по внутрішніх протоколах і через інтерфейси API.

7.1.2 Протоколи взаємодії Softswitch з іншим обладнанням NGN

Обладнання Softswitch може підтримувати наступні види протоколів.

1. При взаємодії з існуючими фрагментами мережі ТфМЗК:
   - безпосередня взаємодія: СКС7 в частині протоколів MTP, ISUP і SCCP;
   - взаємодія через сигнальні шлюзи: M2UA, M3UA, M2PA для передачі сигналізації СКС7 через пакетну мережу;
   - V5UA для передачі сигнальної інформації V5 через пакетну мережу;
   - IUA для передачі сигнальної інформації первинного доступу ISDN через пакетну мережу;
   - MEGACO (H.248) для передачі інформації, що поступає по системах сигналізації по виділених сигнальних каналах (2ВСК). В даний час відомі подібні реалізації в частині системи сигналізації R1; вимог і прикладів реалізації MEGACO для підтримки російської системи сигналізації R1.5 не існує.
2. При взаємодії з термінальним устаткуванням:
   - безпосередня взаємодія з термінальним устаткуванням пакетних мереж: SIP і H.323;
   - взаємодія з устаткуванням шлюзів, що забезпечує підключення термінального устаткування ТфМЗК: MEGACO (H.248) для передачі сигналізації по аналогових абонентських лініях; IUA для передачі сигнальної інформації базового доступу ISDN.
3. При взаємодії з іншими Softswitch: SIP-T.
4. При взаємодії з устаткуванням інтелектуальних платформ (SCP): INAP.

5. При взаємодії з серверами застосувань: в даний час така взаємодія, як правило, базується на внутріфірмових протоколах, в основі яких лежать технології JAVA, XML, SIP і ін.
6. При взаємодії з устаткуванням транспортних шлюзів:
   - для шлюзів, що підтримують транспорт IP або IP/ATM: H.248, MGCP, IPDC і др.;
   - для шлюзів, що підтримують транспорт ATM: BICC.

Основні типи сигналізації, які використовує Softswitch:

- сигналізація для управління з'єднаннями;
- сигналізація для взаємодії різних Softswitch між собою;
- сигналізація для управління транспортними шлюзами.

Основними протоколами сигналізації для управління з'єднаннями є:

- SIP;
- H.323;
- ОКС-7.

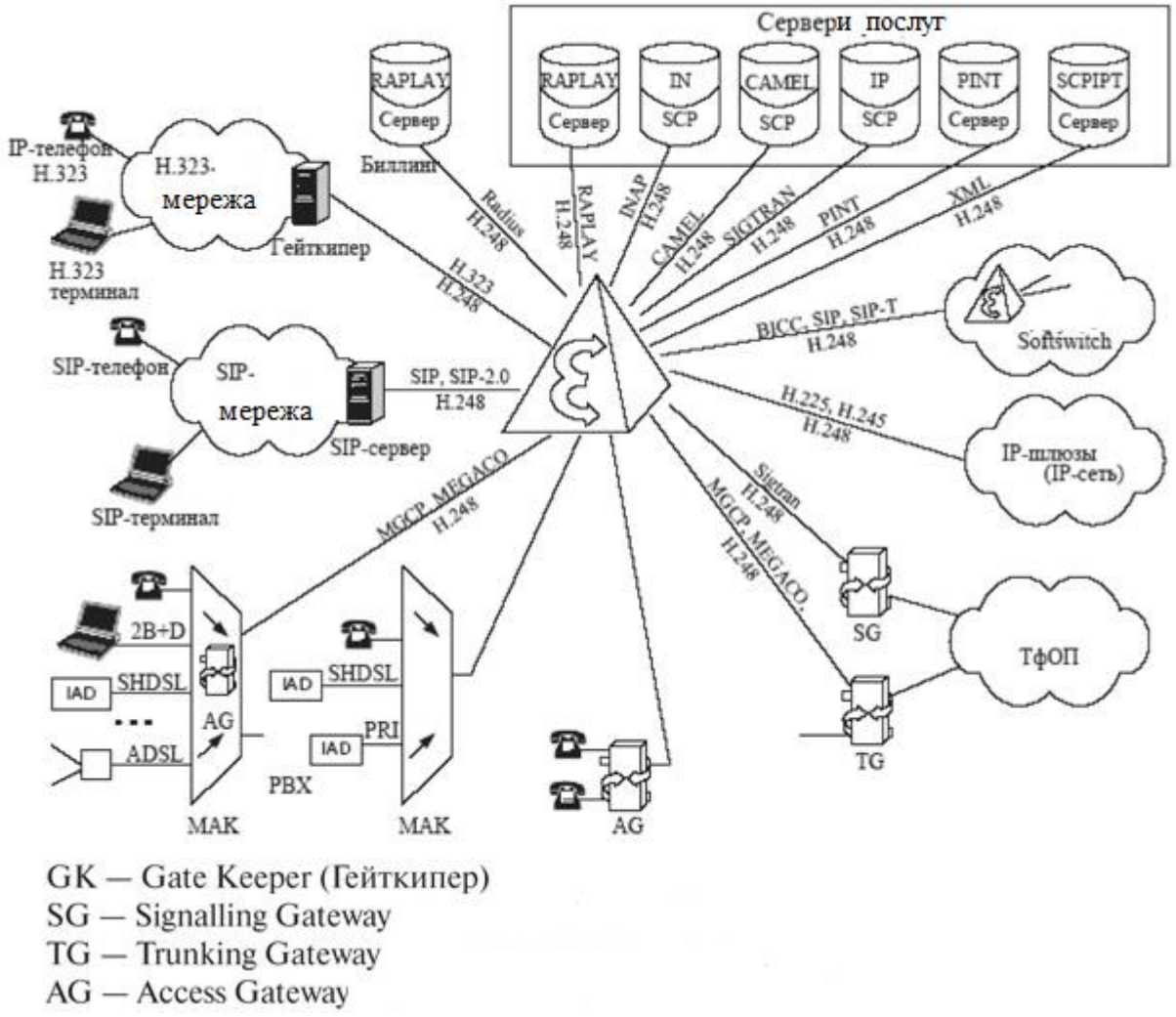


Рис. 7.2 - Взаємодія Softswitch з іншим обладнанням

Також опціонально використовуються:

- абонентська сигналізація E-DSS-1 первинного доступу ISDN;
- протокол абонентського доступу через інтерфейс V5;

Таблиця 7.1. Основні протоколи взаємодії Softswitch з іншим обладнанням NGN

Протокол	Функція в мережі NGN	Коментар
SIP	Управління і встановлення сеансу зв'язку	Застосовується для встановлення як голосових, так і мультимедійних викликів по IP-мережам. Використовує дуже багато напрацьованих механізмів, прийнятих в Інтернеті, і вважається простішим порівняно з протоколом H.248. Термінальні пристрої містять програмне забезпечення SIP-агента. Інтелектуальність зміщується від опорної мережі до абонентських пристроїв.
SIP-T	Передача сигналізації ТфМЗК ISUP через SIP-сеть	Спеціальний різновид протоколу SIP, що забезпечує «прозору» передачу повідомлень ISUP по мережі SIP. Фактично SIP-мережа виконує в цьому випадку функцію транзитного пункту сигналізації. Робота по стандартизації продовжується для забезпечення всієї функціональності, прийнятої в ТфМЗК
H.323	Управління і встановлення сеансу зв'язку	Найбільш поширений протокол в мережах передачі голосу по IP. Вважається важко масштабованим і менш перспективним в порівнянні з протоколом SIP.
H.248/Megaco	Управління шлюзами доступу в пакетну мережу	Найбільш перспективний стандарт, що розробляється. Потенційно повинен забезпечити набагато більші можливості по сумісності різного устаткування
MGCP	Управління шлюзами доступу в пакетну мережу	Не дивлячись на те, що існують мережі з використанням даного протоколу, подальша робота по його розвитку бачиться проблематичной через особливості протоколу
BICC	Управління викликом в мережах з розділеними рівнями управління і перенесення інформації	Протокол встановлення з'єднання, не залежний від типа використовуваної мережі перенесення (IP, ATM). Реалізує повний набір послуг ТфМЗК/ISDN. Містить комплект стандартів, що описують не лише сигнальні процедури, але і мережну архітектуру. Основна ідея протоколу - забезпечити повну реалізацію всіх прийнятих голосових послуг класичної телефонії при використуванні пакетних мереж. Прийнятий 3GPP для мереж мобільного зв'язку 3G

SIGTRAN	Передача протоколів управління і сигналізації по IP-мережі	Набор стандартів, пропонованих IETF для забезпечення надійної передачі сигналізації по IP-мережі (транспортування інформації сигналізації)

Основними протоколами сигналізації управління транспортними шлюзами є:

- MGCP;
- MEGACO/H.248.

Основними протоколами сигналізації взаємодії між Softswitch:

- SIP-T
- BICC.

Основні протоколи взаємодії Softswitch з іншим обладнанням NGN представлені в таблиці 7.1.

7.1.2.1 Протокол H.323

Для побудови мереж IP-телефонії першою стала рекомендація H.323 ITU-T, яка є також першою зонтичною специфікацією систем мультимедійного зв'язку для роботи в мережах з комутацією пакетів, що не забезпечують гарантовану якість обслуговування (рис. 7.3).

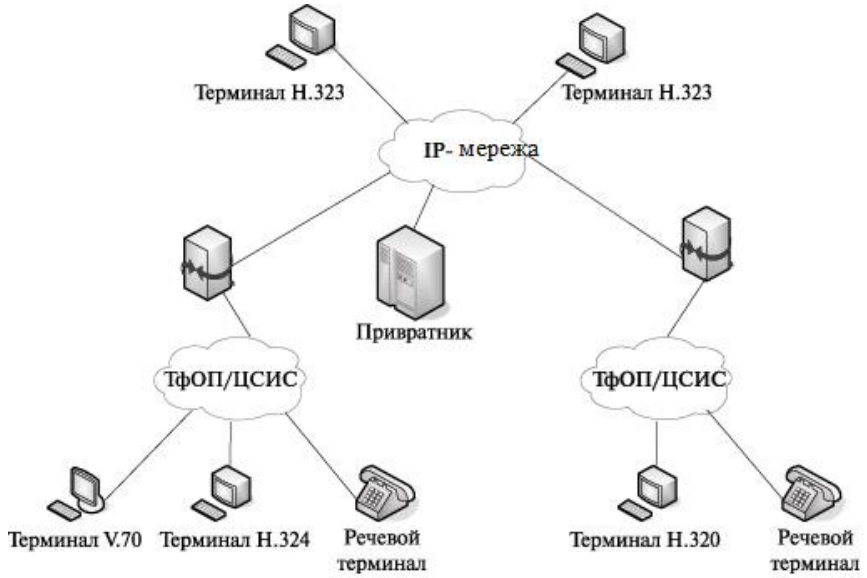


Рис. 7.3.- Структура мережі H.323

Мережі, побудовані на базі протоколів H.323, орієнтовані на інтеграцію з телефонними мережами і можуть розглядатися як мережі ISDN (цифрова мережа з інтеграцією служб), накладені на мережі передачі даних. Зокрема, процедура встановлення з'єднання в таких мережах IP-телефонії базується на рекомендації ITU-T Q.931 і практично ідентична тій же процедурі в мережах ISDN. При цьому рекомендація H.323 передбачає застосування всіляких алгоритмів стискування мовної інформації, що дозволяє використовувати смугу

пропускання ресурсів передачі набагато ефективніше, ніж в мережах з комутацією каналів.

Основними пристроями мережі є: термінал, шлюз, гейткипер (сторож). На відміну від пристроїв ТФМЗК, пристрої Н.323 не мають жорстко закріпленого місця в мережі, а підключаються до будь-якої точки IP-мережі. Проте при цьому мережа Н.323 розбивається на зони, а кожною зоною управляє сторож.

- Термінал Н.323 – кінцевий пристрій мережі IP-телефонії, що забезпечує 2-сторонній мовний або мультимедійний зв'язок з іншим терміналом, шлюзом або пристроєм управління конференціями.
- Шлюз є сполучаючим мостом між ТфМЗК і IP. Основна функція шлюзу – перетворення мовної (мультимедійною) інформації, що поступає з боку ТфМЗК з постійною швидкістю, у вигляд, придатний для передачі по IP-мережам, тобто кодування інформації, придушення пауз в розмові, упаковка інформації в пакети RTP/UDP/IP, а також зворотне перетворення. Крім того, шлюз повинен перетворювати аналогову абонентську сигналізацію, сигналізацію по 2ВСК і повідомленнях систем сигналізацію DSS1 і ОКС7 в сигнальні повідомлення Н.323. За відсутності в мережі сторожа має бути реалізована ще одна функція шлюзу: перетворення номера ТФМЗК в транспортну адресу IP-мережі.
- Гейткіпер (Gatekeeper) виконує функції управління зоною мережі IP-телефонії, в яку входять термінали і шлюзи, зареєстровані у даного гейткіпера. Різні ділянки зони мережі Н.323 можуть бути територіально рознесені, але з'єднуватися один з одним через маршрутизатори.

У число найбільш важливих функцій, що виконуються гейткіпером, входять:

- перетворення alias-адреса (імені абонента, телефонного номера, адреси електронної пошти і ін.) в транспортну адресу мереж з маршрутизацією пакетів IP (IP-адрес і номер порту RTP);
- контроль доступу користувачів системи до послуг IP-телефонії за допомогою сигналізації RAS (Registration, Admission and Status);
- контроль, управління і резервування пропускної спроможності мережі;
- маршрутизація сигнальних повідомлень між терміналами, розташованими в одній зоні.

Гейткіпер також забезпечує для користувача можливість дістати доступ до послуг будь-якого терміналу в будь-якому місці мережі і здатність мережі ідентифікувати користувачів при їх переміщенні з одного місця в інше.

7.1.2.2 Протокол SIP

Другим варіантом побудови мереж IP став протокол SIP, розроблений комітетом IETF (Internet Engineering Task Force); специфікації протоколу представлені в документі RFC 2543.

Протокол ініціації сеансів – Session Initiation Protocol (SIP) – є протоколом прикладного рівня і призначається для організації, модифікації і завершення сеансів зв'язку: мультимедійних конференцій, телефонних з'єднань і розподілу мультимедійної інформації, в основу якого закладені наступні принципи:

- персональна мобільність користувачів. Користувачеві привласнюється унікальний ідентифікатор, а мережа надає йому послуги зв'язку незалежно від того, де він знаходиться;
- масштабованість мережі (характеризується в першу чергу можливістю збільшення кількості елементів мережі при її розширенні);
- розширюваність протоколу характеризується можливістю доповнення протоколу новими функціями при введенні нових послуг і його адаптації до роботи з різними застосуваннями.

Протокол SIP може бути використаний спільно з протоколом H.323. Можливо також взаємодія протоколу SIP з системами сигналізації ТфМЗК – DSS1 і СКС7.

Однією з найважливіших особливостей протоколу SIP є його незалежність від транспортних технологій. Як транспорт можуть застосовуватися протоколи X.25, Frame Relay, AAL5, IPX і ін. Структура повідомлень SIP не залежить від вибраної транспортної технології. Але в той же час перевага віддається технології маршрутизації пакетів IP і протоколу UDP. Приклад побудови мережі SIP представлений на рис. 7.4.

Мережа SIP містить наступні основні елементи.

- Агент користувача (User Agent або SIP client) є застосуванням термінального устаткування і включає дві складові: клієнт агента користувача (User Agent Client – UAC) і сервер агента користувача (User Agent Server – UAS), інакше званий клієнт і сервер. Клієнт UAC ініціює SIP-запити, тобто виступає як зухвала сторона. Сервер UAS приймає запити і відповідає на них, тобто виступає як сторона, що викликається.
- Запити можуть передаватися не прямо адресатові, а на деякий проміжний вузол (проксі-сервер і сервер переадресації).
- Проксі-сервер (proxy server) приймає запити, обробляє їх і відправляє далі на наступний сервер, який може бути як іншим проксі-сервером, так і останнім UAS. Таким чином, проксі-сервер приймає і відправляє запити і клієнта, і сервера. Прийнявши запит від UAC, проксі-сервер діє від імені цього UAC.

- Сервер переадресації (redirect server) передає клієнтові відповідає на запит адреса наступного сервера або клієнта, з яким перший клієнт зв'язується потім безпосередньо. Він не може ініціювати власні запити. Адреса повідомляється першому клієнтові в полі Contact повідомлень SIP. Таким чином, цей сервер просто виконує функції пошуку поточного адреса користувача.
- Сервер місцерозташування (location server) розташування – база адрес, доступ до якої мають SIP-сервери, що користуються її послугами для отримання інформації про можливе місце розташування користувача, що викликається. Прийнявши запит, сервер SIP звертається до сервера місцерозташування, аби взнати адрес, за яким можна знайти користувача. У відповідь той повідомляє або список можливих адресів, або інформує про неможливість знайти їх.

Для організації взаємодії з існуючими застосуваннями IP-сетей і забезпечення вищезазначеної мобільності користувачів протокол SIP використовує принцип адресації, подібний до електронної пошти. Як адреси використовуються спеціальні універсальні покажчики ресурсів URL (Universal Resource Locators), звані SIP URL.

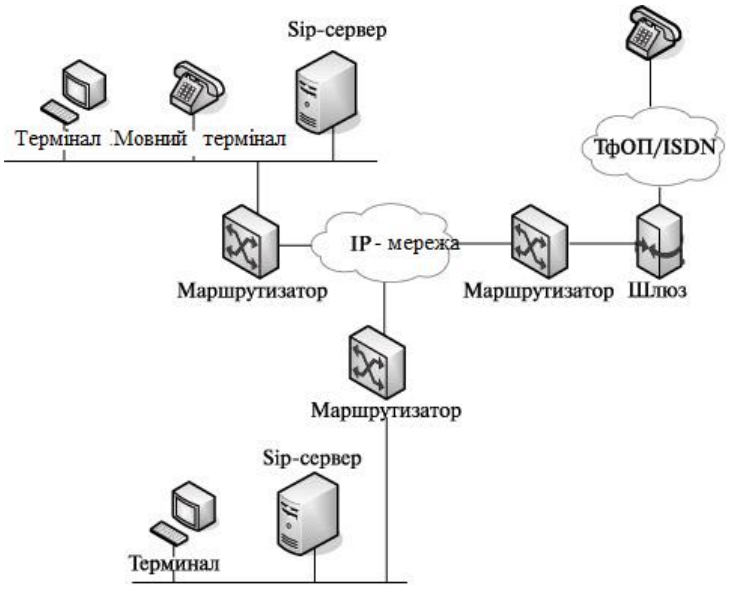


Рис. 7.4. Приклад побудови SIP-мережі

Розрізняються SIP-адреса наступних типів:

- ім'я@домен
- ім'я @хост
- ім'я @IP-адрес
- № телефону@шлюз.

SIP-адрес складається з двох частин. Перша частина адреси – це ім'я користувача, зареєстрованого в домені мережі або на робочій станції. Якщо

друга частина адресу ідентифікує який-небудь шлюз, то в першій вказується телефонний номер абонента.

У другій частині адреси вказується ім'я домена мережі, хоста або шлюзу. Для визначення IP-адреса пристрою необхідно звернутися до служби доменовых імен DNS (Domain Name Service). Якщо ж в другій частині SIP-адреса розміщується IP-адрес, то з робочою станцією можна зв'язатися безпосередньо.

На початку адресу ставляться ключове слово, наприклад ’sip:’, вказуюче, що це саме SIP URL. Існують також інші URL (наприклад, ‘tel:’). Нижче наводяться приклади SIP-адресів:

sip: alex@niits.ru
sip: boris@218.10.12.123
tel: +78129998877@sip-gateway.ru

7.1.2.3 Протокол MGCP

Робоча група MEGACO комітету IETF розробила протокол управління шлюзами – Media Gateway Control Protocol (MGCP).

При розробці протоколу управління шлюзами робоча група MEGACO спиралася на принцип декомпозиції, згідно якому шлюз розбивається на окремі функціональні блоки (рис. 7.5):

- транспортний шлюз – Media Gateway, який виконує функції перетворення мовної інформації, що поступає з боку ТфМЗК з постійною швидкістю, у вигляд, придатний для передачі по мережах з маршрутизацією пакетів IP: кодування і упаковку мовної інформації в пакети RTP/UDP/IP, а також зворотне перетворення;
- пристрій управління – Call Agent, що виконує функції управління шлюзом;
- шлюз сигналізації – Signaling Gateway, який забезпечує доставку сигнальній інформації, що поступає з боку ТфМЗК, до пристрою управління шлюзом і перенесення сигнальної інформації у зворотному напрямі.

Таким чином, весь інтелект функціонально розподіленого шлюзу розміщується в пристрої управління, функції якого у свою чергу можуть бути розподілені між декількома комп'ютерними платформами. Шлюз сигналізації виконує функції STP – транзитного пункту системи сигналізації по загальному каналу – СКС7. Транспортні шлюзи виконують лише функції перетворення мовної інформації. Один пристрій управління обслуговує одночасно декілька шлюзів. У мережі може бути присутніми декілька пристроїв управління. Передбачається, що ці пристрої синхронізовані між собою і погоджено управляють шлюзами, що беруть участь в з'єднанні. Робоча група MEGACO не

визначає протокол синхронізації роботи пристроїв управління, проте у ряді робіт, присвячених дослідженню можливостей протоколу MGCP, для цієї мети пропонується використовувати протоколи H.323, SIP або ISUP/IP.

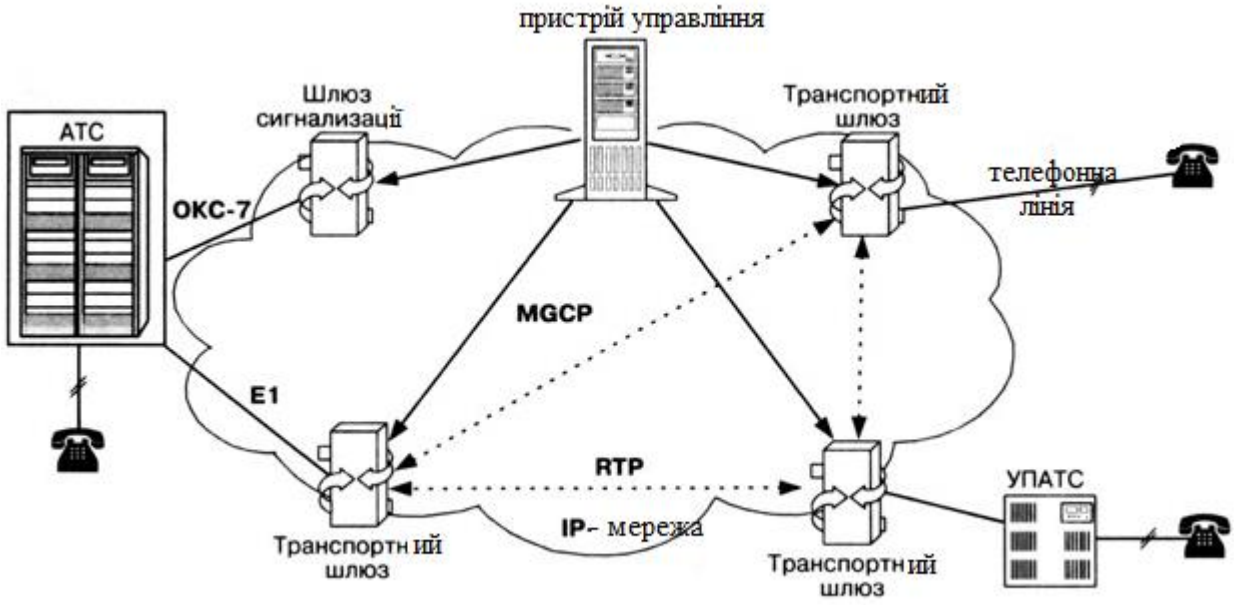


Рис. 7.5 - Архітектура мережі, що базується на протоколі MGCP

Перенесення повідомлень протоколу MGCP забезпечує протокол UDP. Одна з основних вимог, що пред'являються до протоколу MGCP, полягає в тому, що пристрої, що реалізовують цей протокол, повинні працювати в режимі без збереження інформації про послідовність транзакцій між пристроєм управління і транспортним шлюзом, тобто в пристроях не вимагається реалізації кінцевого автомата для опису цієї послідовності.

Протокол MGCP є внутрішнім протоколом, що підтримує обмін інформацією між функціональними блоками розподіленого шлюзу. Протокол MGCP використовує принцип master/slave (ведучий/ведений), причому пристрій управління шлюзами є ведучим, а транспортний шлюз – веденим пристроєм, який виконує команди, що поступають від пристрою управління.

Таке рішення забезпечує масштабованість мережі і простоту експлуатаційного управління нею через пристрій управління шлюзами. До того ж неінтелектуальні шлюзи вимагають меншої продуктивності процесорів і, як наслідок, виявляються менш дорогими. Крім того, забезпечується можливість швидко додавати нові протоколи сигналізації і нові додаткові послуги, оскільки потрібні для цього зміни зачіпають лише пристрій управління шлюзами, а не самі шлюзи.

Робочою групою MEGACO запропонована наступна класифікація транспортних шлюзів (Media Gateways):

- Trunking Gateway – шлюз між ТфМЗК і мережею з маршрутизацією пакетів IP, орієнтований на підключення до телефонної мережі за

допомогою великої кількості цифрових трактів (від 10 до декількох тисяч) з використанням системи сигналізації СКС 7;

- Voice over ATM Gateway – шлюз між ТФМЗК і АТМ-мережею, який також підключається до телефонної мережі за допомогою великої кількості цифрових трактів (від 10 до декількох тисяч);
- Residential Gateway – шлюз, що підключає до IP-мережі аналогові, кабельні модеми, лінії xDSL і широкосмугові пристрої безпровідного доступу;
- Access Gateway – шлюз для підключення до мережі IP-телефонії невеликої установчо-виробничої АТС через аналоговий або цифровий інтерфейс;
- Business Gateway – шлюз з цифровим інтерфейсом для підключення до мережі з маршрутизацією IP-пакетів установчо-виробничої АТС при використанні, наприклад, системи сигналізації DSS1;
- Network Access Server – сервер доступу до IP-мережі для передачі даних;
- Circuit switch або packet switch – комутаційні пристрої з інтерфейсом для управління від зовнішнього пристрою.

7.1.2.4 Протокол MEGACO/H.248

Робоча група MEGACO комітету IETF, продовжуючи дослідження, направлені на удосконалення протоколу управління шлюзами, створила більш функціональний (в порівнянні з розглянутим в попередньому пункті протоколом MGCP) протокол MEGACO. Але розробкою протоколів управління транспортними шлюзами, окрім комітету IETF, займалася ще і дослідницька група SG 16 Міжнародного союзу електрозв'язку. Специфікації адаптованого протоколу приведені в рекомендації ITU-T H.248.

Розглянемо коротко основні особливості протоколу MEGACO/H.248. Для перенесення сигнальних повідомлень MEGACO/H.248 можуть використовуватися протоколи UDP, TCP, SCTP або транспортна технологія ATM. Підтримка для цих цілей протоколу UDP – одна з обов'язкових вимог до контролера шлюзів. Протокол TCP повинен підтримуватися і контролером, і транспортним шлюзом, а підтримка протоколу SCTP, так само як і технології ATM, є необов'язковою.

При описі алгоритму встановлення з'єднання з використанням протоколу MEGACO комітет IETF спирається на спеціальну модель процесу обслуговування виклику, відмінну від моделі MGCP. Протокол MEGACO оперує з двома логічними об'єктами усередині транспортного шлюзу: порт (termination) і контекст (context), якими може управляти контролер шлюзу (рис. 7.6).

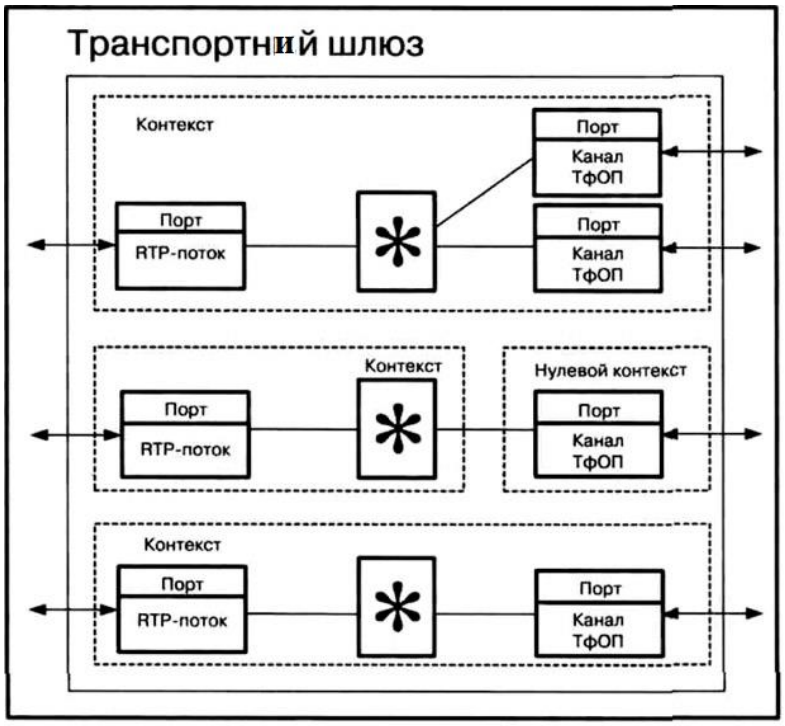


Рис. 7.6. Приклади моделі процесу обслуговування виклику

Порти є джерелами і приймачами мовної інформації. Визначено два види портів: фізичні і віртуальні.

Фізичні порти, що існують постійно з моменту конфігурації шлюзу, - це аналогові телефонні інтерфейси устаткування, що підтримують одне телефонне з'єднання, або цифрові канали, що також підтримують одне телефонне з'єднання і згруповані за принципом часового розділення каналів в тракт E1.

Віртуальні порти, що існують лише протягом розмовної сесії, є портами з боку IP-мережі (RTP-порти), через які ведуться передача і прийом пакетів RTP.

Контекст – це відображення зв'язку між декількома портами, тобто абстрактне представлення з'єднання двох або більш за портів одного шлюзу. У будь-який момент часу порт може відноситися лише до одного контексту, який має свій унікальний ідентифікатор. Існує особливий вигляд контексту – нульовий. Всі порти, що входять в нульовий контекст, не зв'язані ні між собою, ні з іншими портами. Наприклад, абстрактним представленням вільного (не зайнятого) каналу в моделі процесу обслуговування виклику є порт в нульовому контексті.

Порт має унікальний ідентифікатор (TERMINATIONID), який призначається шлюзом при конфігурації порту. Наприклад, ідентифікатором порту може служити номер тракту E1 і номер часового каналу усередині тракту.

За допомогою протоколу MEGACO контролер може змінювати властивості портів шлюзу. Властивості портів групуються в дескриптори, які включаються в команди управління портами.

7.1.2.5 Транспортування інформації сигналізації (SIGTRAN)

Транспортування інформації сигналізації за технологією SIGTRAN призначене для передачі повідомлень протоколу сигналізації мережі з комутацією каналів через мережу з комутацією пакетів і повинна забезпечувати:

- передачу повідомлень різноманітних протоколів сигналізації, обслуговуючих з'єднання мереж з комутацією каналів (CSN), наприклад протоколів прикладних і призначених для користувача підсистем СКС7 (включаючи рівень 3 MTP, ISUP, SCCP, TCAP, MAP, INAP і т. д.), а також повідомлень рівня 3 протоколів DSS1/PSS1 (тобто Q.931 і QSIG);
- засоби ідентифікації конкретного протоколу сигналізації мережі, що транспортується, з комутацією каналів;
- загальний базовий протокол, що визначає формати заголовків, розширення в цілях інформаційної безпеки і процедури для транспортування сигнальної інформації, а також (при необхідності) розширення для введення конкретних індивідуальних протоколів сигналізації мережі з комутацією каналів;
- функціональні можливості (за участю мережного протоколу, що пролягає нижче, наприклад IP), відповідні нижньому рівню конкретної мережі з комутацією каналів.

7.1.3 Обладнання, з яким взаємодіє Softswitch

Як правило, обладнання Softswitch підтримує наступні види інтерфейсів:

- інтерфейс E1 (2048 Кбіт/с) для підключення сигнальних каналів СКС7, що включаються безпосередньо в Softswitch ;
- інтерфейси сімейства Ethernet для підключення до IP-мережі. Через Ethernet-інтерфейси передається сигнальна інформація у напрямі пакетної мережі.

Шлюзи (Gateways) – пристрої доступу до мережі і сполучення з існуючими мережами. Устаткування шлюзів реалізує функції по перетворенню сигнальної інформації мереж з комутацією каналів в сигнальну інформацію пакетних мереж, а також функції по перетворенню інформації транспортних каналів в пакети IP/чарунки ATM і маршрутизації пакетів IP/чарунок ATM. Шлюзи функціонують на транспортному рівні/рівні доступу.

Для реалізації можливості підключення до мультисервісної мережі різних видів обладнання ТфМЗК використовуються різні програмні і апаратні конфігурації шлюзового устаткування:

- транспортний шлюз (Media Gateway (MG)) – реалізація функцій перетворення мовної інформації в пакети IP/чарунки ATM і маршрутизації пакетів IP/чарунок ATM;
- сигнальні шлюзи (Signalling Gateway (SG)) – реалізація функції перетворення систем міжстанційної сигналізації мережі СКС7 (квазізв'язний режим) в системи сигналізації пакетній мережі (SIGTRAN (MXUA));
- транкинговый шлюз (Trunking Gateway (TGW)) – спільна реалізація функцій MG і SG;
- шлюз доступу (Access Gateway (AGW)) – реалізація функції MG і SG для устаткування доступу, що підключається через інтерфейс V5;
- резидентний шлюз доступу (Residential Access Gateway (RAGW)) – реалізація функції підключення користувачів, що використовують термінальне устаткування ТфМЗК/ISDN до мультисервісної мережі.

Обладнання транспортного шлюзу повинне виконувати функції пристрою, що проводить обробку інформаційних потоків середовища передачі.

Обладнання транспортного шлюзу повинне реалізовувати наступний перелік обов'язкових функцій:

- функцію адресації: забезпечує привласнення адресів транспортування IP для засобів прийому і передачі;
- функцію транспортування: забезпечує погоджене транспортування потоків середовища передачі між доменом IP і доменом мережі з комутацією каналів, включаючи, наприклад, виконання процедур перетворення кодувань і ехокомпенсації;
- функцію трансляції кодека: маршрутизує інформаційні транспортні потоки між доменом IP і доменом мережі з комутацією каналів;
- функцію забезпечення секретності каналу середовища передачі: гарантує секретність транспортування інформації у напрямі до шлюзу і від шлюзу;
- функцію транспортного закінчення мережі з комутацією каналів: включає реалізацію процедур всіх низькорівневих апаратних засобів і протоколів мережі;
- функцію транспортного закінчення мережі пакетної комутації: включає реалізацію процедур всіх протоколів, задіяних в розподілі транспортних ресурсів, на мережі пакетної комутації, у тому числі процедури використання кодеків;
- функцію обробки транспортного потоку з пакетною комутацією/комутацією каналів: забезпечує перетворення між каналом передачі аудіоінформації, каналом передачі факсимільної інформації або каналом передачі даних на стороні мережі з комутацією каналів і

пакетами даних (наприклад RTP/UDP/IP або ATM) на стороні мережі пакетної комутації;

- функцію надання каналу для послуги: забезпечує такі послуги, як передача повідомлень і тональних сигналів у напрямі до мережі з комутацією каналів або до мережі пакетної комутації;
- функцію реєстрації використання: визначає і реєструє інформацію об сигналізації і інформацію про прийом або передачу повідомлень, передаваних в транспортних потоках;
- функцію інформування про використання: повідомляє зовнішній об'єкт про поточне і зареєстроване використання (ресурсів);
- функцію OAM&P: експлуатація, управління (адміністрування), технічне обслуговування і надання тій інформації, яка не потрібна безпосередньо для управління викликом і може передаватися до системи управління елементами через логічно окремий інтерфейс;
- функцію менеджменту: забезпечує взаємодію з системою менеджменту мережі.

Обладнання сигнального шлюзу повинне виконувати функції посередника при сигналізації між пакетною мережею і мережею з комутацією каналів.

Обладнання сигнального шлюзу сигналізації повинне реалізовувати наступний перелік обов'язкових функцій:

- функцію закінчення протоколів рівня, розташованого нижче рівня протоколу управління викликом мережі з комутацією каналів;
- функцію секретності сигнальних повідомлень: забезпечує секретність сигнальних повідомлень у напрямі до шлюзу і від шлюзу ;
- функцію OAM&P: експлуатація, управління (адміністрування), технічне обслуговування і надання тій інформації, яка не потрібна безпосередньо для управління викликом і може передаватися до системи управління елементами через логічно окремий інтерфейс;
- функцію менеджменту: забезпечує взаємодію з системою менеджменту мережі.

Обладнання шлюзів може підтримувати наступні протоколи.

1. Для транспортних шлюзів:
    - у напрямі до Softswitch: H.248, MGCP, IPDC для управління викликами при використанні транспортної технології IP; BICC для управління викликами при використанні транспортної технології ATM;
    - у напрямі до інших шлюзів або термінального обладнання пакетної мережі: RTP, RTCP при використанні транспортної технології IP; PNNI або UNI при використанні ATM.

2. Для сигнальних шлюзів:
    - у напрямі до мережі ТфМЗК: залежно від реалізації можлива підтримка рівня MTP2 або MTP3 системи сигналізації СКС7. У першому випадку сигнальний шлюз повинен термінувати рівень MTP3 і передавати всю "вищестоящу" інформацію у напрямі Softswitch з використанням протоколу M2UA. У другому випадку сигнальний шлюз повинен термінувати рівень MTP3 і передавати "вищестоящу" інформацію у напрямі Softswitch з використанням протоколу M3UA;
    - у напрямі до Softswitch: залежно від використовуваних механізмів обробки СКС7 можуть підтримуватися M2UA або M3UA.
3. Для шлюзів доступу:
    - у напрямі до Softswitch для передачі сигнальної інформації, пов'язаної з обслуговуванням виклику: V5UA при підключенні обладнання мережі доступу: MEGACO (H.248) при підключенні абонентів, що використовують сигналізацію по аналоговій абонентській лінії; IUA при підключенні абонентів, що використовують базовий доступу ISDN. Для передачі сигнальної інформації управління шлюзами: H.248, MGCP, IPDC;
    - у напрямі до інших шлюзів і термінального обладнання пакетної мережі: RTP, RTCP;
    - у напрямі до ТФМЗК: сигналізацію по аналогових абонентських лініях, сигналізацію базового доступу ISDN в частині протоколів рівня 2 (LAP-D), сигналізацію по інтерфейсу V5 в частині протоколів рівня 2 (LAP-V5).

Як правило, обладнання шлюзів підтримує наступні інтерфейси:

1. Транспортні шлюзи:
    - у напрямі до ТФМЗК підтримують інтерфейси PDH (E1) і SDH (STM1/4). У напрямі пакетної мережі на основі IP-технологій: інтерфейси Ethernet.
2. Сигнальні шлюзи:
    - у напрямі ТФМЗК в основному підтримують інтерфейс PDH (E1), а у напрямі пакетної мережі – інтерфейс 10Base Ethernet:
3. Шлюзи доступу:
    - у напрямі ТФМЗК підтримують інтерфейс по аналогових абонентських лініях, інтерфейси базового доступу ISDN (U, S, S-T) для резидентних шлюзів і інтерфейс PDH (E1) і шлюзів доступу, що здійснюють підключення обладнання інтерфейсу V5. У напрямі пакетної мережі на основі IP технологій:

інтерфейси 10-100Base Ethernet. У напрямі пакетної мережі на основі ATM технологій: UNI.

З точки зору технічних характеристик (у пакетній частині), для такого обладнання визначаються вимоги по ємкості, продуктивності, надійності, підтримуваним протоколам і реалізованим інтерфейсам до пакетної мережі.

Термінальне обладнання – термінальні пристрої, використовувані для надання голосових і мультимедійних послуг зв'язку і призначені для роботи в пакетних мережах.

Існує два основні типи термінальних пристроїв, призначених для роботи в пакетних мережах: SIP-термінали і H.323-термінали. Дане обладнання може мати як спеціалізоване апаратне (standalone), так і програмного виконання (softphone).

Також інколи використовується термінальне обладнання на основі протоколу MEGACO. Таке термінальне обладнання поєднує в собі функції аналогового телефонного апарату і шлюзу доступу в частині перетворення сигналізації по аналогових абонентських лініях. Його функціональні можливості обмежуються можливостями аналогового апарату, але воно може безпосередньо підключатися до пакетної мережі.

Ще одним виглядом термінального обладнання є інтегровані пристрої доступу (IAD). Як правило, IAD забезпечує підключення термінального обладнання мереж ТФМЗК (аналогові ТА і термінали ISDN) і термінального обладнання мереж передачі даних. У IAD реалізуються функції по перетворенню протоколів сигналізації ТФМЗК в протоколи пакетних мереж (SIP/H.323) і перетворенню потоків призначеної для користувача інформації між мережами з комутацією каналів і пакетними мережами. Найближча аналогія з IAD в мережах ТФМЗК – обладнання установчо-виробничих автоматичних телефонних станцій (УВАТС).

Термінальне обладнання підтримує протоколи SIP або H.323 у напрямі Softswitch для передачі інформації сигналізації і управління комутацією і протоколи RTP/RTCP для передачі призначеної для користувача інформації. Для підключення до мережі, як правило, застосовується інтерфейс Ethernet.

Сервер застосувань – використовується для надання розширеного списку додаткових послуг абонентам пакетних мереж. Сервери застосувань призначені для виконання функцій рівня послуг і управління послугами.

Специфікація виконуваних функцій залежить від групи послуг, що реалізовується за допомогою сервера послуги, і не може бути сформульована на абстрактному рівні.

Сервери застосувань, як правило, взаємодіють з обладнанням Softswitch, де задіяні технології Java, XML, SOAP. Підключення проводиться в основному з використанням інтерфейсів, що базуються на Ethernet.

7.2 Концепція IP multimedia subsystem (IMS)

Концепція IP Multimedia Subsystem (IMS) описує нову мережну архітектуру, основним елементом якої є пакетна транспортна мережа, що підтримує всі технології доступу і що забезпечує реалізацію великого числа інфокомунікаційних послуг. Її авторство належить міжнародному партнерству Third Generation Partnership Project (3GPP).

IMS спочатку розроблялася для побудови мобільних мереж 3-го покоління на базі протоколу IP. Надалі концепція була прийнята Комітетом ETSI-TISPAN, зусилля якого були направлені на специфікацію протоколів і інтерфейсів, необхідних для підтримки і реалізації широкого спектру послуг в стаціонарних мережах з використанням стека протоколів IP.

В даний час архітектура IMS розглядається багатьма операторами і сервіс-провайдерами, а також постачальниками обладнання як можливе рішення для побудови мереж наступного покоління і як основа конвергенції мобільних і стаціонарних мереж на платформі IP.

Причину виникнення концепції IMS саме в середовищі розробників стандартів для мобільних мереж можна пояснити таким чином. Останніми роками оператори стаціонарних мереж активно підтримують перехід від традиційних телефонних мереж до NGN, пов'язуючи з ними певні надії на скорочення операційних витрат і капітальних вкладень, а також на розвиток нових послуг, чекаючи, як наслідок, істотного підвищення доходів. Природно, ідея побудови NGN виявилася привабливою і для мобільних операторів, які останніми роками зіткнулися з різким падінням доходів, що зв'язане, у тому числі, і з дерегулюванням ринку, зростанням конкуренції, тарифними війнами, високим відтоком абонентів і так далі.

Проте слід визнати, що основна технологічна ідея NGN – розділення транспортних процесів і процесів управління викликами і сеансами на базі елементів платформи Softswitch – не була підтримана своєчасною розробкою відповідного набору стандартів. Це привело до того, що основні мережні елементи NGN, що поставляються різними виробниками, частенько виявляються несумісними між собою.

У мережах мобільних операторів, де одним з основних джерел доходів є роумінг, така несумісність виявляється куди значнішим недоліком, ніж в стаціонарних мережах. Саме це і визначило активність міжнародних організацій (в першу чергу ETSI і 3GPP), які почали розробку нових принципів побудови і стандартів мобільних мереж 3G, грунтуючись на рівневій архітектурі NGN.

По суті концепція IMS виникла в результаті еволюції мереж UMTS, коли область управління мультимедійними викликами і сеансами на базі протоколу SIP додали до архітектури мереж 3G. Серед основних властивостей архітектури IMS можна виділити наступні:

- багаторівневість – розділяє рівні транспорту, управління і застосувань;
- незалежність від середовища доступу – дозволяє операторам і сервіс-провайдерам конвергувати фіксовані і мобільні мережі;
- підтримка мультимедійного персонального обміну інформацією в реальному часі і аналогічного обміну інформацією між людьми і комп'ютерами (наприклад ігри);
- повна інтеграція мультимедійних застосувань реального і нереального часу (наприклад потокові застосування і чати);
- можливість взаємодії різних видів послуг;
- можливість підтримки декількох служб в одному сеансі або організації декількох одночасних синхронізованих сеансів.

7.2.1 Стандартизація IMS

Стандартизація архітектури IMS є предметом уваги широкого круга міжнародних організацій, завдяки ключовій ролі IMS в еволюції мереж у напрямі до NGN. Концепція IMS в її справжньому вигляді є, головним чином, результатом робіт трьох міжнародних організацій по стандартизації – 3GPP, 3GPP2 і ETSI.

Партнерство 3GPP було створене в кінці 1998 р. за ініціативою інституту ETSI з метою розробки технічних специфікацій і стандартів для мобільних мереж зв'язку 3-го покоління (мереж UMTS), що базуються на мережах GSM, які розвиваються. Партнерство 3GPP2 з'явилося в 1998 р. також за ініціативою ETSI і Міжнародного союзу електрозв'язку для розробки стандартів мереж 3G (мережі CDMA-2000) в рамках проекту IMT-2000, створеного під егідою ITU. Воно було утворене практично тими ж організаціями, що і в разі 3GPP. Основним вкладом організації 3GPP2 в розвиток стандартів для мобільних мереж 3G з'явилося поширення концепції IMS на мережі CDMA2000 (IP-транспорт, SIP- сигналізація), описане в специфікації під загальною назвою MultiMedia Domain (MMD). Обоє партнерства розробляють стандарти мереж 3G, орієнтуючись на широке застосування IP-орієнтованих протоколів, стандартизованих Комітетом IETF, і використовуючи основні ідеї архітектури NGN.

Вперше концепція IMS була представлена в документі 3GPP Release 5 (березень 2002 р.), де була сформульована основна її мета – підтримка мультимедійних послуг в мобільних мережах на базі протоколу IP, а також

специфіковані механізми взаємодії мобільних мереж 3G на базі архітектури IMS з безпроводовими мережами 2G.

Архітектура мереж 3G відповідно до концепції IMS має декілька рівнів (площин) з розділенням по рівнях транспорту, управління викликами і застосувань. Підсистема IMS має бути повністю незалежна від технологій доступу і забезпечувати взаємодію зі всіма існуючими мережами – мобільними і стаціонарними, телефонними, комп'ютерними і так далі.

У документі 3GPP Release 6 (грудень 2003 р.) ряд положень концепції IMS були уточнені, додані питання взаємодії з безпроводовими локальними мережами і захисту інформації (використання ключів, абонентських сертифікатів).

У релізах 6 і 7 визначена ідеологія здійснення IP-комунікацій за допомогою SIP. Відповідно до неї SIP починається безпосередньо з мобільного терміналу.

Специфікація Release 7 додає дві основні функції, які є ключовими в стаціонарних мережах:

- Network Attachment, яка забезпечує механізм аутентифікації абонентів і необхідна в стаціонарних мережах, оскільки в них відсутні SIM-карти ідентифікації користувача;
- Resource Admission, що резервує мережні ресурси в стаціонарних мережах для забезпечення сеансів зв'язку.

Роботи, направлені на розширення концепції IMS на стаціонарні мережі, проводяться Комітетом TISPAN. Інтерес до архітектури IMS з боку ETSI привів до створення нової робочої групи (2003 р.), що об'єднала відому групу TIPHON (Telecommunications and Internet Protocol Harmonization Over Networks) і Технічний комітет SPAN (Services and Protocols for Advanced Networks), який відповідає за стандартизацію стаціонарних мереж.

Нова група, що отримала назву TISPAN (Telecommunications and Internet converged Services and Protocols for Advanced Networking), відповідає за стандартизацію сучасних і перспективних конвергованих мереж, включаючи VoIP і NGN, а також все, що пов'язане з архітектурою IMS.

7.2.2 Архітектура IMS

Рекомендація Y.2021 ITU-T дає наступне визначення IMS:

Мультимедійна IP-подсистема (IMS) – це комплекс функціональних елементів базової мережі, призначений для надання послуг на базі протоколу SIP. IMS підтримує реєстрацію користувача і кінцевого пристрою на певній

ділянці мережі. В якості однієї з дій реєстрації IMS виконує аутентифікацію і інші дії із забезпечення безпеки.

Принцип, на якому будується концепція IMS, полягає в тому, що доставка будь-якої послуги жодним чином не співвідноситься з комунікаційною інфраструктурою (за винятком обмежень по пропускній спроможності). Втіленням цього принципу є багаторівневий підхід, використовуваний при побудові IMS. Він дозволяє реалізувати незалежний від технології доступу відкритий механізм доставки послуг, який дає можливість впроваджувати в мережі застосування сторонніх постачальників послуг.

У складі IMS виділяються три рівні (площини): транспортний рівень (рівень користувача, user plane), рівень управління (control plane) і рівень послуг (застосувань, application plane).

Необхідно відзначити, що архітектура IMS специфікує не вузли мережі, а функції. Це означає, що IMS-архітектура, як і Softswitch, теж є набором функцій, з'єднаних стандартними інтерфейсами. Розробники мають право комбінувати декілька функцій в одному фізичному об'єкті або, навпаки, реалізувати одну функцію розподілено, проте найчастіше фізичну архітектуру ставлять у відповідність функціональної і реалізують кожну функцію в окремому вузлі.

Різні функції IMS зв'язуються одна з однією через набір контрольних точок, еталонні точки в IMS використовуються для ідентифікації і опису інтерфейсів між різними функціональними мережними елементами.

На рисунках 7.7 і 7.8 представлена архітектура IMS різного ступеню деталізації.

Розглянемо основні функціональні компоненти архітектури IMS.

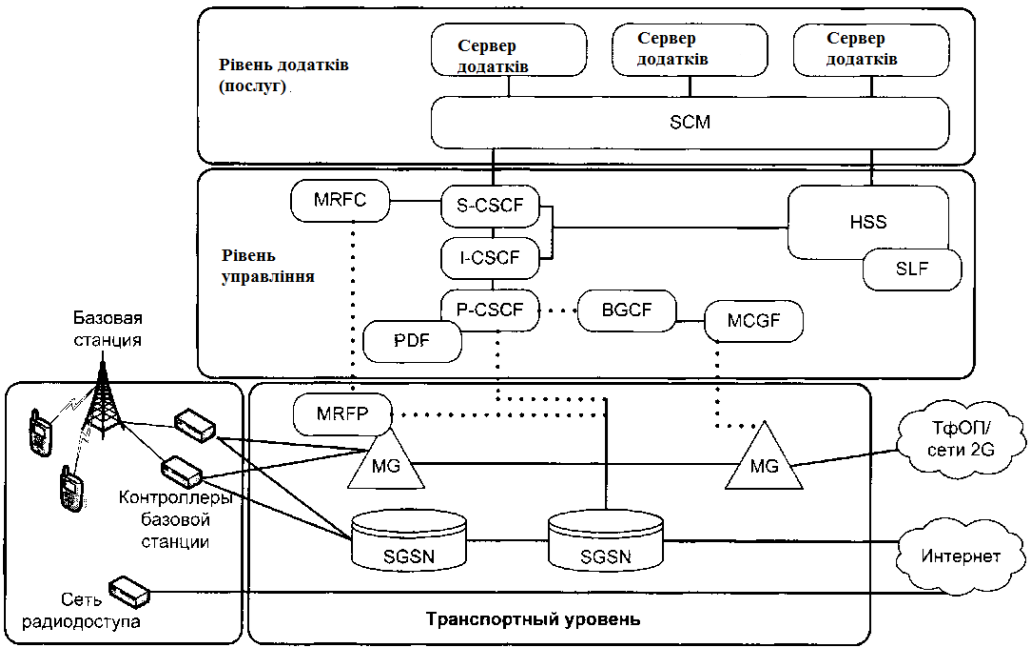


Рис. 7.7. Архітектура підсистеми IMS

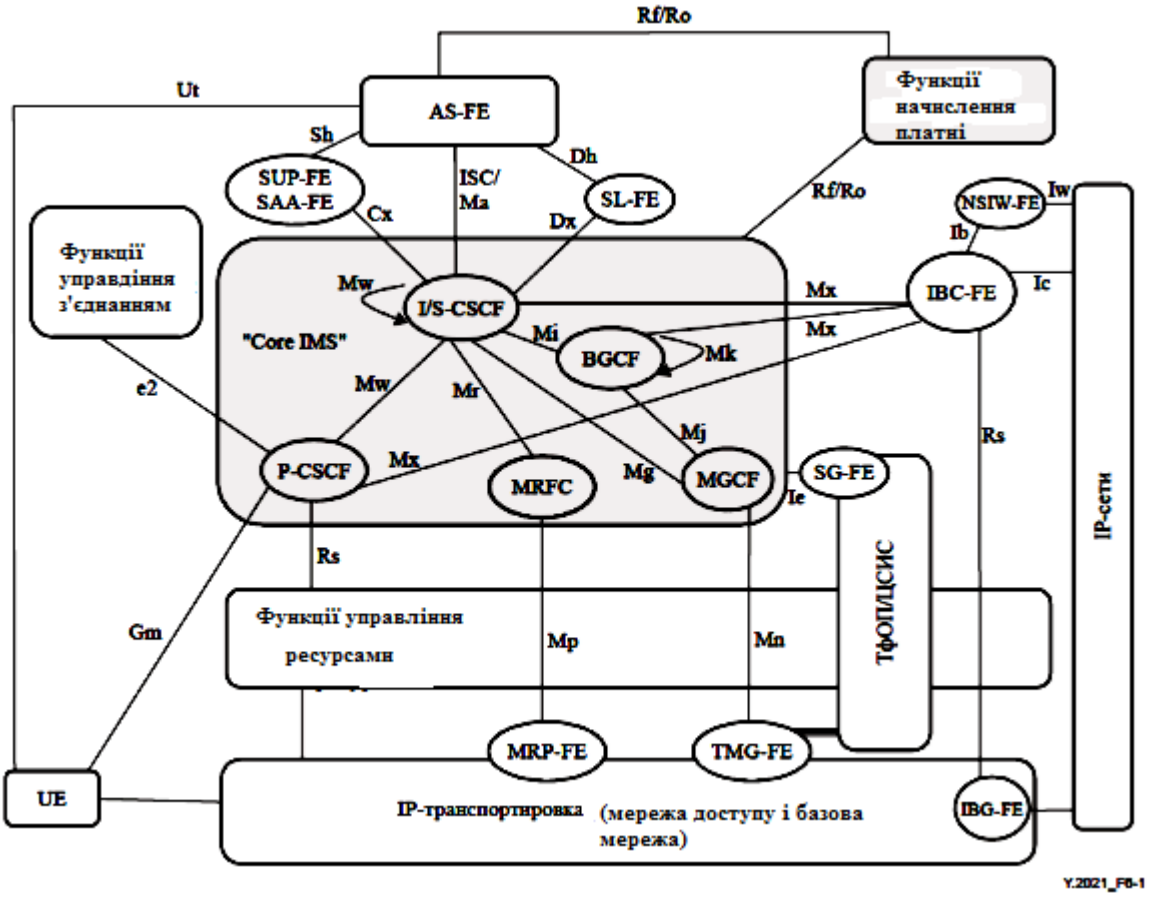


Рис. 7.8. Архітектура підсистеми IMS

7.2.2.1 Функціональні блоки площини управління

CSCF - Call Session Control Function - функція управління сеансом зв'язку встановлює, контролює, підтримує і припиняє мультимедійні сеанси зв'язку, а також управляє взаємодією послуг користувача.

CSCF є основною на площині управління IMS -платформи. Модуль CSCF, використовуючи протокол SIP, виконує функції, що забезпечують доставку множини послуг реального часу за допомогою транспорту IP. Функція CSCF використовує динамічну інформацію для ефективного управління мережними ресурсами (граничні пристрої, шлюзи і сервери застосувань) залежно від профілю користувачів і застосувань. Модуль CSCF включає три основні функції:

- P-CSCF - Proxy CSCF – проксі-CSCF – через неї в систему IMS поступає весь призначений для користувача трафік;
- I-CSCF - Interrogating CSCF – запрошуюча CSCF – є точкою з'єднання з домашньою мережею. I-CSCF звертається до HSS, аби знайти S-CSCF для конкретного абонента;
- S-CSCF - Serving CSCF – обслуговуюча CSCF – обробляє всі SIP-повідомлення, якими обмінюються кінцеві пристрої;

Розглянемо детальніше ці функціональні блоки.

Кожна сигнальна подія, яка генерує користувач, спершу вирушає до проксі-CSCF (P-CSCF) незалежно від самої сигнальної події, яка може передбачати такі речі як запит сеансу зв'язку, активізацію необхідної функції, виділення мережного ресурсу, запит обслуговування іншим застосуванням. Таким чином, функція P-CSCF є першим контактом для пристрою користувача в IMS-ядрі.

Отримавши повідомлення SIP від користувачевого пристрою, P-CSCF пересилає їх функції Interrogating Call Session Control Function (I-CSCF) або функції Serving Call Session Control Function (S-CSCF). Функція I-CSCF служить єдиною точкою реєстрації в мережі для доступу до послуг IMS як для місцевих, так і роумінгових користувачів. Як тільки I-CSCF реєструє користувача, S-CSCF вступає у володіння і управляє сеансом зв'язку, забезпечуючи доступ до всіх потрібних служб.

P-CSCF є початковою точкою взаємодії (на сигнальному рівні) користувачевого IMS-термінала і IMS-мережі. Вона може бути розташована в різних місцях, в межах домашньої мережі або в межах гостьової мережі.

З точки зору SIP вона є вхідним/вихідним проксі-сервером, через який проходять всі запити, що виходять від IMS-термінала або направляються до нього. Проте P-CSCF може поводитися і як агент користувача UA, що необхідне для переривання сеансів в нестандартних ситуаціях, і для створення незалежних SIP-транзакцій, пов'язаних з процесом реєстрації.

P-CSCF прикріпляється до терміналу користувача при реєстрації в мережі і не замінюється протягом всього терміну реєстрації. Основним призначенням P-CSCF є маршрутизація запитів і відповідей SIP між користувачевим терміналом і вузлами IMS-мережі (I-CSCF, S-CSCF і ін.).

P-CSCF виконує також ряд вимог, що відносяться до забезпечення захисту. Вона встановлює декілька асоціацій IPsec (Асоціація захисту – Security Association - є погодженою політикою або способом обробки даних, обмін якими передбачається між двома пристроями сторін, що спілкуються), що забезпечують цілісність інформації, передаваної до IMS-терміналу. Створення цих асоціацій передбачає аутентифікацію користувача, і виконавши її, P-CSCF сповіщає про цього користувача останні вузли мережі, аби їм не потрібно було повторно виконувати ту ж процедуру.

У завдання P-CSCF входить і перевірка правильності побудови повідомлень SIP, передаваних IMS-терміналом. Крім того, P-CSCF проводить компресію і декомпресію повідомлень SIP для того, щоб прискорити час їх передачі по вузькосмугових каналах (наприклад, на радіоділянці) і, тим самим, зменшити час встановлення з'єднання або надання послуги. Крім того, P-CSCF виявляє запити з'єднань з аварійними службами і або повідомляє про помилку, або вибирає S-CSCF, необхідну для організації такого зв'язку. Ще одним

завданням P-CSCF є створення облікової інформації і відправка її до вузла, що відповідає за нарахування плати. Аби забезпечувалися масштабованість і надійність, IMS-мережа зазвичай містить декілька P-CSCF, кожна з яких обслуговує деяку кількість IMS-терміналів, залежну від ємкості вузла. IMS-архітектура передбачає, що P-CSCF може знаходитися як в домашній, так і в гостьовій мережі. Якщо мережа базується на технології GPRS, то P-CSCF повинна знаходитися там же, де і GGSN (Gateway GPRS Support Node), тобто в домашній мережі, але у міру поширення IMS ця умова не буде обов'язковою для обох вузлів.

Вибір QoS і управління QoS є ще однією функцією, яку P-CSCF може виконувати як складову частину свого процесу реалізації політики. В межах цієї області відповідальності у нього є можливість вибирати потрібні варіанти політики використання застосування і ресурсів мережі, авторизувати доступ до мережних ресурсів, управляти QoS. Нарешті, в P-CSCF є можливість збирати дані, які потрібні для функцій білінгу.

I-CSCF - основне завдання цього блоку – ідентифікація привілеїв зовнішнього абонента щодо доступу до послуг, вибір відповідного сервера застосувань і забезпечення доступу до нього

I-CSCF взаємодіє по протоколу Diameter з користувачевими базами HSS і SLF, отримує від них інформацію про місцезнаходження користувача і про обслуговуючу його S-CSCF. Якщо S-CSCF ще не призначена, I-CSCF проводить її призначення. Додатково I-CSCF може шифрувати частини SIP-повідомлень, що містять важливу інформацію про домен, таку як кількість серверів в домені, їх DNS-імена і тому подібне. Ця група функцій називається THIG (Topology Hiding Inter-network Gateway) - міжмережний шлюз приховання топології.

Підтримка THIG опціональна і не завжди потрібна; зокрема вона не потрібна, якщо провайдер на границі своєї мережі встановлює граничний контролер SBC (Session Border Controller). Зазвичай, аби забезпечувалася масштабованість і надійність, в мережі присутні декілька I-CSCF. Типовим місцезнаходженням I-CSCF є домашня мережа, проте у ряді специфічних випадків, таких як підтримка THIG, вона може бути винесена і в гостьову мережу.

S-CSCF – обслуговуюча функція S-CSCF – центральна інтелектуальна функція на сигнальному рівні, тобто функція SIP-сервера, який управляє сеансом. Окрім функції SIP-сервера, S-CSCF виконує функцію реєструючого сервера мережі SIP (SIP-registrar), тобто підтримує прив'язку місцезнаходження користувача (наприклад, IP-адресом терміналу, з якого користувач дістав доступ в мережу) до його SIP-адресу PUI (Public User Identity).

Аналогічно I-CSCF, S-CSCF взаємодіє по протоколу Diameter з HSS, отримує від нього дані аутентифікації користувача, що намагається дістати

доступ до мережі, і дані про профіль користувача, тобто перелік доступних йому послуг – набір тригерних точок для маршрутизації повідомлення SIP до серверів застосувань. У свою чергу, S-CSCF інформує HSS про те, що цей користувач прикріплений до нього на термін своєї реєстрації, і про спрацьовування таймера реєстрації.

Вся сигнальна інформація SIP, що передається і приймається користувачевим IMS-терміналом, проходить через S-CSCF, до якої прикріплений користувач. S-CSCF аналізує кожне повідомлення і визначає, чи повинне воно, на шляху до пункту призначення, пройти через сервери застосувань, що надають користувачеві послуги.

S-CSCF підтримує сеанс протягом всього часу його продовження і, у міру потреби, взаємодіє з сервісними платформами і з функціями нарахування плати. Однією з основних функцій S-CSCF є маршрутизація SIP-повідомлень. Якщо користувач набирає телефонний номер замість SIP URI, то S-CSCF проводить перетворення номера формату E.164 відповідно до RFC3761. Для забезпечення масштабованості і надійності в мережі можуть знаходитися декілька S-CSCF, причому вони завжди розташовуються в домашній мережі.

PDF - Функція Policy Decision Function - інколи інтегрується з P-CSCF, але може бути реалізована окремо. Ця функція відповідає за формування політики на підставі інформації про характер сеансу і про переданий трафік (транспортні адреса, ширина смуги і так далі), отриманої від P-CSCF. На базі цієї інформації PDF приймає рішення про авторизацію запитів від GGSN і проводить повторну авторизацію при зміні параметрів сеансу, а також може заборонити передачу певного трафіку або організацію сеансів деяких типів.

BGCF - Breakout Gateway Control Function – функція управління шлюзами, управляє пересилкою викликів між доменом комутації каналів (ТФМЗК або GSM) і мережею IMS. Даний модуль здійснює маршрутизацію на основі телефонних номерів і вибирає шлюз в домені комутації каналів, через який мережа IMS (де розташований сервер BGCF) взаємодіятиме з ТФМЗК або GSM. Тут також проводиться генерація відповідних облікових записів для нарахування плати абонентам мереж з комутацією каналів.

MGCF - Media Gateways Control Function – функція управління шлюзами (Media Gateways) – управляє з'єднаннями в транспортних шлюзах IMS, використовуючи протоколи H.248/MEGACO;

MRFC - Media Resource Function Controller - знаходиться на сигнальному рівні і взаємодіє з S-CSCF по протоколу SIP. Використовуючи отримані інструкції, MRFC управляє по протоколу MEGACO/H.248 процесором MRFP (Media Resource Function Processor), що знаходиться на рівні передачі даних, а

той виконує всі маніпуляції з медіа-інформацією. Самі MRF завжди знаходяться в домашній мережі.

IBCF - Interconnect Border Control Function - забезпечує керованість на границі між мережами різних провайдерів. Вона може містити в собі THIG, виконує узгодження IPv4 і IPv6, може, у разі потреби, звертатися до функції IWF (InterWorking Function – взаємодія з іншими IP-мережами), може управляти доступом і призначати смугу пропускання відповідно до власної політики або звертаючись до підсистеми RACS (Resource and Admission Control Subsystem - управління доступом до ресурсів).

На рисунках 7.7 і 7.8 показаний набір функціональних елементів, які утворюють підсистему IMS, але не показаний можливий розподіл цих елементів в мережі реєстрації абонента і у відвідуваній мережі NGN. На рисунку 7.9 показані елементи управління сеансом зв'язку IMS разом з вказуванням базових мереж, усередині яких вони можуть знаходитися.

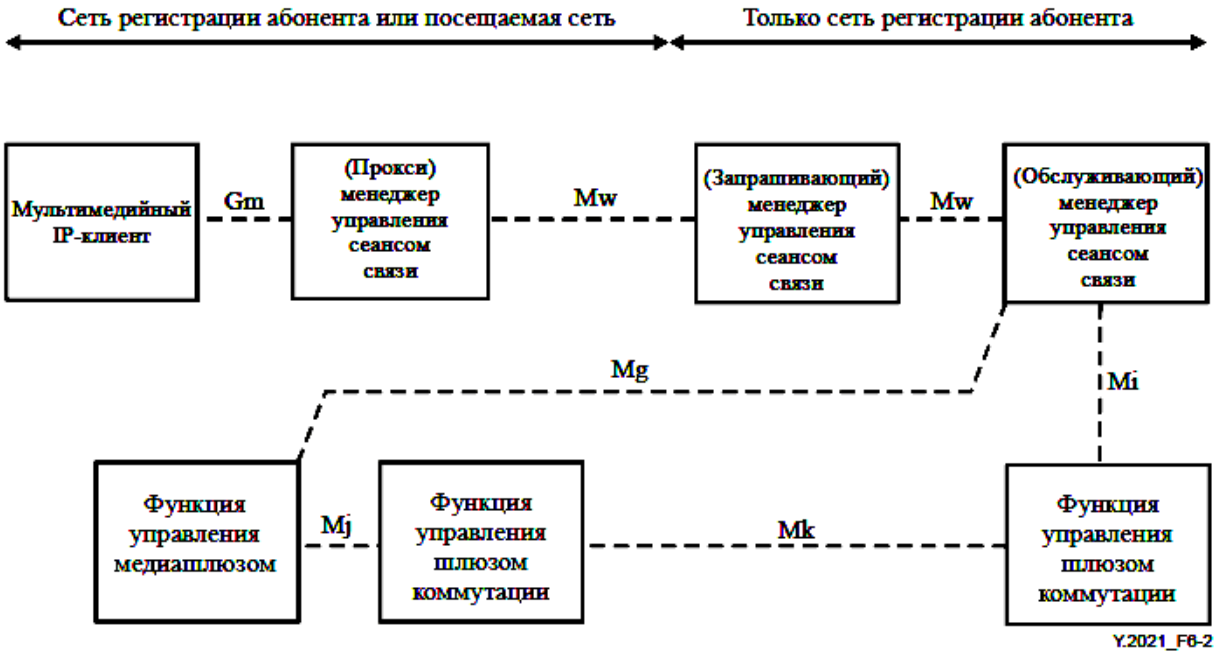


Рис. 7.9. Взаємозв'язок елементів управління сеансом зв'язку з базовими мережами

Як показано на рисунку 7.9, перший елемент управління сеансом зв'язку протоколу SIP (P-CSCF) і контрольна точка з'єднання з ТФМЗК можуть підтримуватися і у відвідуваній мережі, і в мережі реєстрації абонента за умови, що між операторами існують відповідні ділові взаємини. Проте функція S-CSCF, яка управляє доступом до послуг IMS, завжди знаходиться в мережі реєстрації абонента.

7.2.2.2 Функціональні блоки площини транспорту (користувача)

Транспортний рівень відповідає за підключення абонентів до інфраструктури IMS за допомогою користувачевого обладнання (User Equipment – UE). В ролі даного обладнання можуть виступати будь-який термінал IMS (наприклад телефон (смартфон) 3G, КПК з підтримкою Wi-Fi, або ж широкосмуговий доступ). Також можливе підключення через шлюзи ні-IMS терміналів (наприклад термінали ТФМЗК).

Розглянемо основне обладнання транспортної площини.

MRF (Media Resource Function) – медіасервер - складається з процесора мультимедійних ресурсів MRFP (Media Resource Function Processor) і контролера MRFC;

MRFP – процесор MRFP – розподіляє медіаресурси мережі згідно командам від MRFC. Його основними функціями є обслуговування потоків мультимедійних даних для служб сповіщення, об'єднання вхідних мультимедіа потоків; обробка потоків мультимедійних даних.

MGW (Media GateWay) – транспортний шлюз – забезпечує пряме і зворотне перетворення потоків RTP в потоки мереж з комутацією каналів (ТФМЗК);

I-BGF (Interconnect Border Gateway Function) – міжмережний граничний шлюз – забезпечує взаємодію між мережами IPv4 і IPv6. Відповідає за забезпечення функцій безпеки (трансляцію адрес і портів NAPT, функції firewall, інструменти QoS). Управляє передачею даних на 3 і 4 рівнях через границю мереж провайдерів. Ця функція грає роль міжмережного екрану і NAT, вона захищає ядро мережі провайдера, фільтруючи пакети на підставі інформації транспортного рівня. Вона використовує NAPT для приховання транспортних адресів елементів ядра мережі IMS.

GGSN (Gateway GPRS Support Node) – шлюзовий вузол GPRS або вузол маршрутизації – є шлюзом між стільниковою мережею (її частиною – GPRS) і IMS. GGSN містить всю необхідну інформацію про мережі, куди абоненти GPRS можуть діставати доступ, а також параметри з'єднання. Основною функцією GGSN є маршрутизація даних, що йдуть до абонента і від нього через SGSN.

SGSN (Serving GPRS Support Node) – вузол обслуговування абонентів GPRS – основний компонент GPRS-системи щодо реалізації всіх функцій обробки пакетної інформації.

RAN – Radio Access Network – обладнання радіодоступу; забезпечує взаємодію IMS і стільникових телекомунікаційних систем;

PDG (Packet Data Gateway) – пакетний шлюз – даний мережний елемент забезпечує доступ користувачевого обладнання WLAN до IMS. Відповідає за трансляцію віддаленого IP-адреса, реєстрацію користувачевого обладнання в IMS, забезпечує виконання функцій безпеки;

WAG (Wireless Access Gateway) – шлюз безпроводового доступу – забезпечує з'єднання мереж WLAN і IMS.

A-BGF/BAS (Access Border Gateway Function / Broadband Access Switch) – забезпечує доступ широкосмугового користувачевого обладнання до IMS. Виконує функції, аналогічні I-BGF.

DSLAM (Digital Subscriber Line Access Multiplexer) – цифровий абонентський шлюз доступу – забезпечує з'єднання абонентів, що використовують широкосмуговий доступ (стаціонарний, наприклад xDSL, мережі кабельного телебаченняя) до IMS.

7.2.2.3 Функціональні блоки площини застосувань (послуг)

Верхній рівень еталонної архітектури IMS містить набір серверів застосувань, які, в принципі, не є елементами IMS. Ці елементи верхньої площини включають в свій склад як мультимедійні IP-застосування, що базуються на протоколі SIP, так і застосування, що реалізовуються в мобільних мережах на базі віртуального домашнього середовища.

SIP AS (SIP Application Server) – сервер застосувань, служить для виконання послуг, що базуються на протоколі SIP. Всі нові послуги в IMS знаходитимуться саме в сервері SIP AS.

OSA-SCS (Open Service Access – Service Capability Server) – сервер можливих послуг, забезпечує інтерфейс до послуг, що базуються на відкритому доступі до послуг (OSA – Open Service Access). Метою є забезпечення послугам можливості доступу до мережних функцій за допомогою стандартного програмного інтерфейсу застосувань.

IM-SSF (IP Multimedia – Service Switching Function) – сервер комутації послуги, служить для з'єднання підсистеми IMS з послугами в системі пристосованих до користувача застосувань для поліпшення логіки мобільної мережі (CAMEL – Customized Applications for Mobile network Enhanced Logic). Йдеться про послуги, розроблені для глобальної системи мобільного зв'язку GSM. За допомогою функції IM-SSF (функція комутації послуг) використання даних послуг можливе і в IMS.

Сервери застосувань можуть знаходитися або в домашній, або в будь-якій іншій мережі, з якою у провайдера є сервісна угода. Але якщо сервер застосувань знаходиться в зовнішній мережі, він не може мати інтерфейсу з HSS.

Слід зауважити, що IMS передбачає також заснований на SIP єдиний інтерфейс, відомий як інтерфейс IMS Service Control (ISC). Цей інтерфейс ISC

дозволяє застосуванням, розміщеним в Parlay/OSA, SIP і CAMEL, взаємно діяти через інтерфейс з ядром IMS.

7.2.3 Користувачеві бази HSS і SLF

Дві основні мережні бази даних забезпечують підтримку IMS: сервер абонентів домашньої мережі HSS (Home Subscriber Server) і функція місцезнаходження абонента SLF (Subscriber Location Function). Кожна IMS-мережа містить один або більш серверів користувачевих баз даних HSS. По суті, HSS є централізованим сховищем інформації про абонентів і послуги і є еволюційним розвитком HLR (Home Location Register) з архітектури мереж GSM. У HSS зберігається вся інформація про користувача, необхідна мережі для підтримки всіх функцій IMS, пов'язаних з обробкою виклику і встановленням мультимедійного сеансу: інформація про місцезнаходження користувача, інформація для забезпечення захисту (аутентифікація і авторизація), інформація про користувачеві профілі, про обслуговуючу користувача S-CSCF, про тригерні точки звернення до послуг, дані, потрібні для аутентифікації і авторизації користувачевого доступу до послуг.

На основі записів в базі даних ідентифікується, до яких послуг користувач має доступ, з якою мережею він зараз з'єднаний. HSS підтримує також локалізацію користувача подібно до домашнього регістра місце знаходження HLR і візитному регістру місцезнаходження VLR в мобільних системах попередніх поколінь.

Мережа може містити більш одного HSS в тому випадку, якщо кількість абонентів дуже велика, аби підтримуватися одним HSS. Така мережа, разом з декількома HSS, повинна буде мати в своєму складі функцію SLF, що є простою базою даних, яка зберігає дані про відповідність інформації HSS адресам користувачів. Вузол, що передав до SLF запит з адресою користувача, отримує від неї відомості про той HSS, який містить інформацію про цього користувача. Як HSS, так і SLF використовують для взаємодії з іншими елементами IMS протокол Diameter.

7.2.4 Білінг в IMS

В області надання послуг є два визнані варіанти реалізації білінга:

• рекурентний білінг, інколи званий офлайновым або автономним білінгом, що зазвичай застосовується до користувачів, які отримують рахунки кожного місяця за послуги, отримані в попередній розрахунковий період;

• заснований на транзакції білінг, інколи званий онлайновим биллингом або білінгом на основі кредитування, застосовується до

клієнтів з передоплатою, які отримують рахунки за послуги з принципу «транзакція -за- транзакцією».

Можна використовувати і той, і інший принцип в одному сеансі; наприклад, клієнт може платити щомісячно за передачу мови, але може захотіти нарахування плати за ті транзакції, коли він завантажує фільм або викликає розширену послугу.

У тарифікаційних ситуаціях, що існують сьогодні, всі компоненти мережі IMS - різні CSCFs, BGCF, функція управління медіаресурсами MRCF, MGCF, сервери застосувань - збирають інформацію по обліку їх використання, а потім відправляють цю інформацію функції колектора оплати (CCF), яка створює запис даних про нарахування плати і відправляє її білінговій системі, а та, у свою чергу, генерує рахунок для користувача.

У IMS кожному встановленому сеансу привласнюється ідентифікатор оплати IMS (ICID), який однозначно визначає сеанс.

Як і інші комунікаційні функції в межах області IMS, протоколи DIAMETER управляють всіма діями AAA (серверів аутентифікації, авторизації і обліку).

7.2.5 Ідентифікація в IMS

У будь-якій мережі зв'язку необхідна ідентифікація користувачів або користувачевих терміналів для того, щоб встановлювати з'єднання між користувачами, однозначно визначеними за допомогою ідентифікаторів. Крім того, при наданні різних послуг інколи необхідно ідентифікувати самі послуги.

Основним ідентифікатором, що привласнюється користувачеві, є Private User Identity (PrUI). Він має формат NAI (NetworkAccess Identifier), визначений в RFC 2486. Формат виглядає таким чином:

username@operator.com.

Відмітимо, що PrUI використовуються для ідентифікації користувача і для його аутентифікації, але на відміну від телефонних номерів в ТФМЗК, не служать для маршрутизації. Користувачеві не обов'язково знати свій ідентифікатор PRUI, він може зберігатися на ідентифікаційній карті.

Реліз 5 3GPP наказував кожному користувачеві мати один унікальний PRUI, але в релизі 6 це обмеження не існує, і тепер користувач може мати декілька різних PrUI. І хоча на одну ідентифікаційну карту, використовувану в UMTS, як і раніше можна помістити лише один PrUI, користувач може мати декілька таких карт і декілька терміналів, що в

комбінації з використанням іншого ідентифікатора, а саме, Public User Identity (PuUI), надає користувачеві велику гнучкість вибору адресів.

Кожному PrUI оператор ставить у відповідність один або декілька PuUI, що мають формат SIP URI (Uniform Resource Identifier) по RFC 3261 або TEL URL (URL - Uniform Resource Locator- Єдиний покажчик ресурсів) по RFC 2806. У IMS ідентифікатор PUUI використовується для маршрутизації сигнальних SIP-повідомлень і як контактна інформація для інших абонентів.

Коли PuUI представлений у форматі SIP URI, він має вигляд:

sip:alexander@operator.com.

У SIP URI можна помістити телефонний номер:

sip:+7-812-960-6293@operator. com;user=phone.

Цей формат необхідний, оскільки для реєстрації протокол SIP вимагає наявність SIP URI, і, отже, не можна зареєструвати TEL URL, але можна зареєструвати SIP URI, що містить телефонний номер.

З іншого боку, аби користувач міг викликати термінали мережі зв'язку загального користування і приймати виклики від них, він повинен мати TEL URL, що має вигляд:

tel: +1-812- 960-6293.

Таким чином, користувачеві зазвичай потребується мінімум два різних PuUI. Інша причина мати декілька PuUI - приваблива для користувача можливість мати різні номери для різних контактів або послуг.

Ідентифікаційна карта IMS-термінала UICC (Universal Integrated Circuit Card) зберігає один PrUI і, як мінімум, один PuUI. Повна структура взаємозв'язку декілька PrUI і PuUI зберігається в абонентському профілі HSS. Приклад такої структури наведений на рис. 7.10.

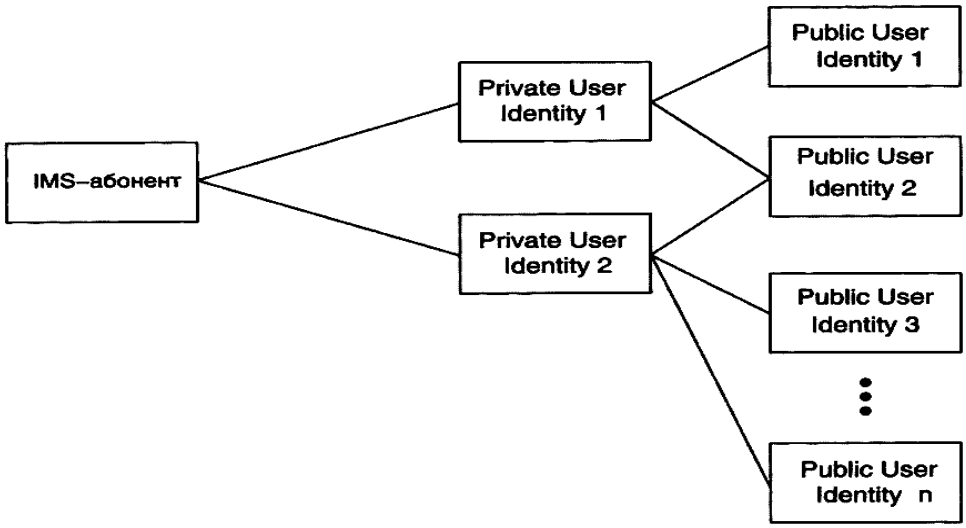


Рис. 7.10. Ідентифікація IMS-абонентів

UICC - термін, що означає змінну ідентифікаційну карту, що має стандартизований інтерфейс з терміналом, а фізично карта UICC може містити декілька логічних застосувань, таких як добре відомий SIM (Subscriber Identity Module), використовуваний при ідентифікації користувачів мереж GSM, USIM (Universal Subscriber Identity Module), який застосовується для ідентифікації в мережах UMTS, і ISIM (IP Multimedia Services Identity Module) - служить для ідентифікації, авторизації і конфігурації терміналу при роботі в IMS-мережі.

Дістати доступ до послуг IMS користувач може лише за умови, що в його UICC міститься USIM або ISIM, причому використання останнього переважно. Структура ISIM приведена на рис. 7.11.

Home Network Domain URI - SIP URI, що визначає ім'я домашньої мережі. Він використовується для пошуку домашньої мережі при реєстрації. У ISIM може зберігатися лише один Home Network Domain URI.

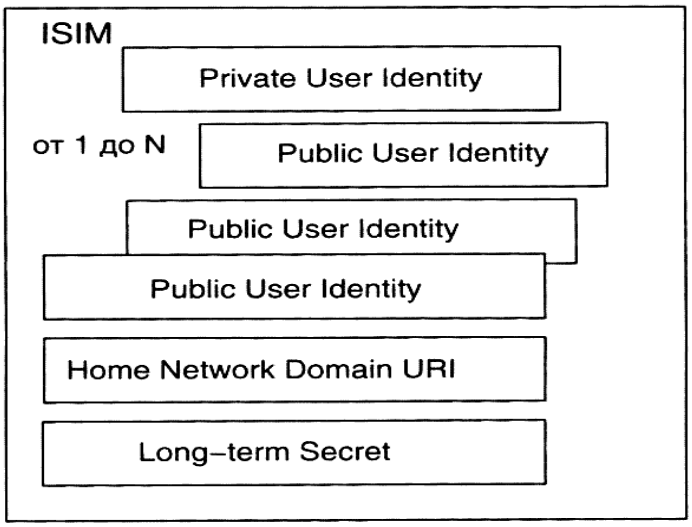


Рис. 7.11. Ідентифікація IMS-абонентів

Long-term Secret - поле, використовуване в цілях аутентифікації, перевірки цілості, розрахунку ключів шифрування. Поля всіх ідентифікаторів доступні терміналу лише для читання.

Ідентифікатор послуги - Public Service Identity (PSI), - з'явився лише в 3GPP Release 6. На відміну від описаних вище ідентифікаторів, PSI привласнюється не користувачам, а послугам, розміщеним на серверах застосувань. Так само, як і PUUI, ідентифікатори PSI можуть мати формат SIP URI або TEL URL.

7.2.6 IMS в стаціонарних мережах

Основним моментом, вигідно відрізняючим IMS від інших концепцій побудови мереж NGN, є якраз наявність стандартів, які дають можливість мати одноманітні і тому здатні ефективно взаємодіяти мережі. До появи архітектури IMS в 3GPP певні роботи велися і в інших і стандартизуючих організаціях. У ETSI і в ITU-T розроблялися елементи архітектури NGN, в IETF стандартизувалися протоколи, в MSF і в IPCC вирішувалися питання по Softswitch, в DSL Forum створювалися специфікації для своєї області, але ніхто не брався за створення цілісної системи. І лише в 3GPP створили завершену систему NGN, концепція якої включає архітектуру, аспекти нарахування плати і білінга, управління, захист інформації, причому все це - з використанням виключно відкритих стандартних інтерфейсів.

Стандартизація використання IMS в стаціонарних мережах і побудови NGN на базі IMS-архітектури ведеться за проектом TISPAN комітету ETSI.

Аналогічно процесу стандартизації і розвитку концепції UMTS-мережі в 3GPP, в TISPAN стандартизація ділиться на етапи, результатом кожного з яких в 3GPP і в TISPAN є черговий реліз.

Так, реліз 3 TISPAN орієнтовано на міжмережну мобільність користувачів і збільшення ширини смуги пропускання в технологіях доступу (VDSL, FTTH, WI-MAX).

Основний упор в релізі 1 TISPAN робиться на використання для доступу до IMS технологій ADSL і WLAN.

Підтримку різнотипного доступу в релізі 1 TISPAN забезпечують дві нові підсистеми:

• Network Attachment Subsystem (NASS) проводить призначення IP-адресов, наприклад, використовуючи протокол DHCP (Dynamic Host Configuration Protocol), аутентифікацію на рівні IP, авторизацію доступу до мережі, визначення місцезнаходження на рівні IP і ін.

• Resource and Admission Control Subsystem (RACS) управляє доступом.

Завдяки спільним зусиллям TISPAN і 3GPP, архітектура IMS адаптується до xDSL доступу, для якого підтримуються мультимедійні послуги, і забезпечується емуляція послуг PSTN/ISDN.

Емуляція полягає в тому, що IP-мережа створює для кінцевого обладнання видимість того, що вона є ТФМЗК/ISDN мережею. Користувачі не відчувають того, що вони підключаються до IP-мережі, а не до ТФМЗК/ISDN, а отже, забезпечується можливість використання і інтелектуальних, і неінтелектуальних терміналів (рис. 7.12).

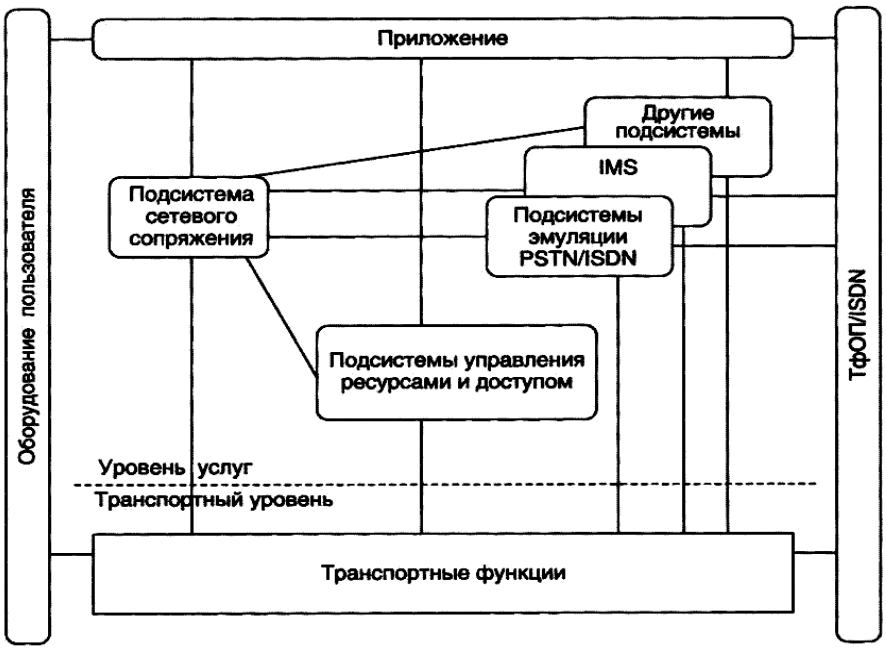


Рис. 7.12. Архітектура мережі NGN в проекті TISPAN

Відмінності між мобільними і стаціонарними мережами в плані реалізації IMS в проекті виглядають наступним образом: існує різниця в ширині смуги, в захисті, в затримках при передачі. До терміналів стаціонарної мережі пред'являються менш строгі вимоги (такі як підтримка IPv6, USIM/ISIM, деяких кодеків). Обладнання користувача стаціонарної мережі не повинне зберігати інформацію про його місцезнаходження, в терміналах стаціонарної мережі немає явного резервування мережних ресурсів; стаціонарні термінали жорстко не прив'язані до користувачів; не реалізується стискування сигнальної інформації; індикація ширини смуги RTCP в SDP зазвичай не потрібна; аутентифікація проводиться без UICC.

7.2.7 Порівняння платформ Softswitch і IMS

Проведемо порівняння Softswitch і IMS. Ці дві архітектури об'єднують такі загальні риси:

- Архітектури Softswitch і IMS має рівневе ділення, причому границі рівнів проходять на одних і тих же місцях. Для архітектури Softswitch описані в першу чергу пристрої мережі, а архітектура IMS визначена на рівні функцій.
- Ідентичні також ідея надання всіх послуг на базі IP-мережі і розділення функцій управління викликом і комутації. По суті, до вже відомих функцій Softswitch додаються функції шлюзу OSA і сервер абонентських даних.

Архітектури Softswitch і IMS мають такі відмінності:

- Незважаючи на то, що склад функцій практично не відрізняється для обох архітектур, є значні відмінності в вмісті кожній з функцій в системах Softswitch і IMS. Окрім того, якщо в архітектурі Softswitch функції мають досить умовне ділення і опис, то в документах IMS дається жорсткий опис функцій і процедур їх взаємодії, а також визначені і стандартизовані інтерфейси між функціями системи.
- Softswitch – це в першу чергу обладнання конвергентних мереж. Функція управління шлюзами (і відповідно протоколи MGCP/MEGACO) є в нім домінуючою (протокол SIP для взаємодії два Softswitch/ MGC). Тоді як IMS проектувалася в рамках мережі 3G, що повністю базується на IP. Основним її протоколом є SIP, що дозволяє встановлювати однорангові сесії між абонентами і використовувати IMS лише як систему, що надає сервісні функції по безпеці, авторизації, доступу до послуг і так далі. Функція управління шлюзами і сам медіашлюз тут лише засіб для зв'язку абонентів 3G з абонентами фіксованих мереж. Причому маються на увазі лише ТФМЗК.
- До особливостей IMS відноситься орієнтованість на протокол IPv6. Можливо, що популярність IMS послужить поштовхом до тривалого впровадження шостої версії протоколу IP. Але доки це представляє деяку проблему: мережі UMTS підтримують і IPv4 і IPv6, тоді як IMS – як правило, лише IPv6. Тому на вході в IMS- заголовків і адресну інформацію. Ця проблема властива не лише IMS, але і всім мережам IPv6.

Однією з сильних сторін платформи Softswitch в даний час є її поширеність: в світі існує множина мереж, що пішли по цьому шляху розвитку, і вже накопичений значний дослідний матеріал по впровадженню SoftSwitch-архітектур. Велика кількість підтримуваних технологій дає можливість операторові підібрати обладнання, що найбільш відповідає його вимогам і що дозволяє оптимальним чином взаємодіяти з вже наявними мережними ресурсами. Рішения SoftSwitch відносно легко масштабувати, починаючи з простої архітектури, обслуговуючої корпоративний сектор, і закінчуючи великомасштабними проектами міжрегіонального оператора. Таким чином, оператор може мінімізувати первинні вкладення в мережу NGN. Ця ж особливість дозволяє операторові, що створює великомасштабний проект, використовувати нові мережні ресурси (і, отже, отримувати прибуток) відразу після їх установки. Якщо узагальнювати перераховані переваги, то їх можна охарактеризувати одним словом – "гнучкість", маючи на увазі під ним адаптацію до будь-яких запитів оператора.

Проте у рішеннях SoftSwitch є і інша сторона. Різноманіття обладнання, представлене в даному сегменті ринку, породжує проблему його сумісності. Багаточисельні центри по забезпеченню системної взаємодії допомагають вирішити її лише частково, оскільки частенько тести не встигають за

оновленням версій програмного забезпечення і не можуть охопити всі можливі комбінації пристроїв, що працюють в мережах операторів. Це також породжує ширшу проблему взаємодії операторів один з одним і зводить нанівець передбачені багатьма технологіями можливості по забезпеченню мобільності користувача і послуг. Деякі виробники обладнання надають фірмові системи управління мережею, які не завжди коректно і повноцінно працюють з обладнанням сторонніх постачальників при його інтеграції в мережу оператора, оскільки є відмінності не лише в реалізації, але і у функціональності багатьох систем.

У IMS частково згладжуються проблеми сумісності обладнання, оскільки взаємодія функціональних модулів регулюється стандартами. Новий підхід до надання послуг виявився надзвичайно вдалим і забезпечив роумінг послуг, що повинне принести додатковий прибуток операторові. Використання в проводових мережах NGN і мобільних мережах 3G уніфікованої системи IMS дозволяє бачити в перспективі можливість конвергенції фіксованих і мобільних мереж – ідеї, що набирає популярність по всьому світу, підтвердженням чому є постійне збільшення учасників FMCA (Fixed-Mobile Convergence Alliance) – міжнародного об'єднання найбільших операторів зв'язку.

Переваги IMS:

- Висока рентабельність обслуговування за рахунок стандартизованої архітектурі IMS.
- Мережа абсолютно не залежить від технології доступу - стирається границя між інфраструктурами фіксованих і мобільних мереж, а також різними сферами надання послуг (телебачення, інформаційні послуги, телекомунікаційні і ін.).
- Унаслідок усунення границі між проводовим і безпроводовим зв'язком, можливість переміщати застосування між цими двома доменами стає набагато простіший, і мобільність може бути включена в існуючі застосування, поширюючи їх за межі границь традиційного проводового зв'язку.
- IMS набагато швидше реагує на замовлення послуги, оскільки інформація про кожного користувача розміщується в єдиному сховищі, що робить бізнес-процеси набагато ефективнішими.
- В порівнянні з так званим безкоштовним мовним зв'язком типа Skype, архітектура IMS має переваги, пов'язані з тим, що IMS привласнює якості обслуговування високий пріоритет. Без IMS передбаченість якості сеансу в Інтернет вельми мала, оскільки часто виявляється неможливим взнати, як джіттер, затримка і втрата пакетів впливатимуть на той або інший сеанс.
- IMS забезпечує збір даних і службу підтримки білінга. Безкоштовні служби VoIP не роблять цього, тоді як IMS не лише може зібрати дані, але і

запропонувати користувачеві безліч опцій білінга. Постачальники послуг можуть використовувати це в своїх інтересах, пропонуючи преміальні послуги (кращий QoS за вищу ціну) або послуги з доданою вартістю, такі як завантажуваний контент, за який можна нараховувати плату окремо.

7.3 Управління мережами NGN

Архітектура мережі NGN, яку було розглянуто в розділі 2, визначає вимоги до моделі системи управління. Архітектура управління NGN згідно з Рекомендацією ITU-T M.3060/Y.2401 (03/06) може бути представлена у вигляді чотирьох різних архітектурних ракурсів, як показано на рисунку 7.13.

- ракурс бізнес-процесів;
- функціональній ракурс управління;
- інформаційній ракурс управління;
- фізичній ракурс управління.

У кожному ракурсі представлені різні точки зору на архітектуру. Для цих чотирьох ракурсів також враховані міркування безпеки.

На рисунку 7.13 зображено послідовність операцій зі створення характеристик управління. Першим визначається функціональний ракурс, за ним – інформаційний ракурс і останім – фізичний ракурс. Бізнес-процеси впливають на інші ракурси протягом всього життєвого циклу. На практиці цей процес є ітеративним, дозволяючи, в міру необхідності, розвиватися всім ракурсам архітектури з часом.

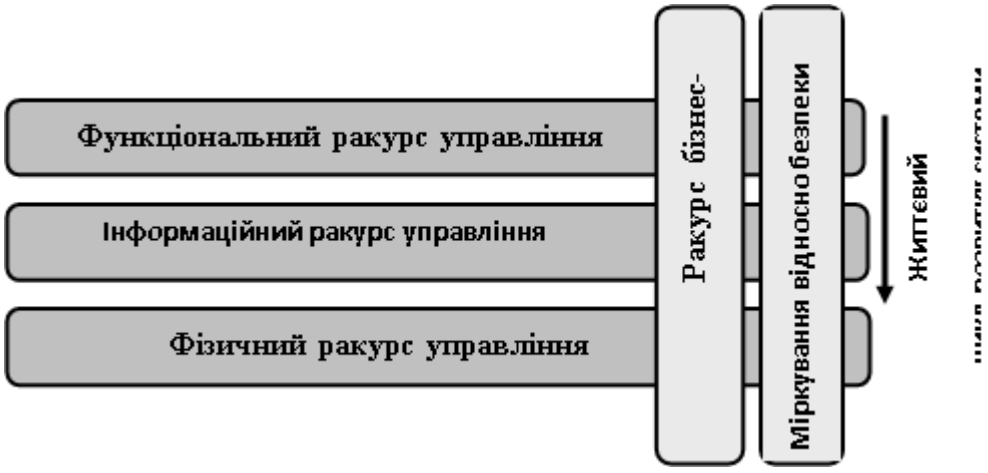


Рис. 7.13. Архітектура управління NGN

Ракурс управління бізнес-процесами ґрунтується на моделі eTOM (MCE-t Рек. серії M.3050.x) і забезпечує еталонну структуру для класифікації діяльності провайдера послуг. Бізнес-процес - це чинник, що робить вплив впродовж всього життєвого циклу системи. Слід взяти до уваги, що на

практиці, цей процес ітеративний, щоб забезпечити розвиток всіх аспектів архітектури в часі.

Функціональна модель визначає перелік функцій, які повинні виконуватися в ході процесу управління.

Інформаційна модель описує інформацію управління, необхідну для зв'язку між об'єктами управління при виконанні функцій згідно з функціональною моделлю архітектури управління.

Фізична модель описує різні способи реалізації функцій управління. Вони можуть бути втілені в різних фізичних конфігураціях, що використовують різні протоколи управління.

Одним з основоположних принципів, які лежать в основі архітектури управління для NGN, є принцип орієнтованості архітектури управління на послуги (SOA- Service-Oriented Architecture).

Сервіс-орієнтовна архітектура - це компонентна модель, яка зв'язує різні сервіси за допомогою чітко певних інтерфейсів і угод між ними. Інтерфейси визначаються незалежним способом, і не залежать від апаратної платформи, операційної системи або мови програмування, на якому реалізований сервіс. Такий підхід дозволяє створювати послуги на різних системах, які взаємодіють один з одним одноманітним і стандартним чином.

Компоненти програми можуть бути розподілені по різних вузлах, і пропонуються як незалежні, слабо зв'язані, замінювані додатки сервісу.

SOA використовує принцип інкапсуляції, орієнтований на об'єкт. При цьому об'єкти можуть бути доступні тільки через інтерфейси і з'єднуються на основі угод про інтерфейс.

У SOA додаток розробляється виходячи з логіки процесу бізнесу. Процес розбивається на деяку послідовність кроків, кожний з яких реалізується як сервісний компонент. І ці компоненти інтегруються так, щоб їх виконання в певній послідовності приводило до потрібного результату.

Таким чином, SOA надає гнучкий метод комбінування і багаторазового використання компонентів для побудови складних розподілених програмних комплексів.

Головні переваги SOA, в порівнянні з іншою архітектурою, що існує раніше, полягають в наступному:

- швидша адаптація до вимог бізнесу, що змінюються;
- скорочення витрат на інтеграцію нових послуг, а також підтримку тих, що існують.

Основні особливості SOA:

- наявність незалежного інтерфейсу, не пов'язаного жорстко з конкретною реалізацією, (*слабкий зв'язок - loose coupling)* між послугами. Гідністю слабозвэ’язаных систем є швидкість і можливість витримувати еволюційні зміни в структурі і реалізації кожного окремо взятого сервісу, які

складають додаток в цілому (жорсткий зв'язок (tight coupling) має на увазі, що інтерфейси різних компонент додатку сильно взаємозв'язані по функціональності і взаємодії, що робить їх достатньо уразливими, коли міняється одна з частин додатку);

- будь-яка дана послуга може приймати роль клієнта або сервера по відношенню до іншої послуги залежно від ситуації;
- парадигма «знайти - пов’язати - виконати» для зв'язку між послугами. Споживач послуг запрошує системний реєстр, що зберігає список доступних послуг, які відповідають його критеріям. Як тільки така послуга знайдена, замовник підключається до послуги, що надається SOA.
- інкапсульований життєвий цикл об'єктів, що беруть участь в транзакціях бізнесу.

SOA передбачає три основні ролі: постачальник послуги (service provider), споживач послуги (service consumer), який потребує певних функцій, що надаються послугою; системний реєстр послуг (registry), виступає як посередник, надаючи каталог з інформацією про всілякі послуги, пропонованих різними постачальниками послуг.

Реєстр містить вичерпну інформацію по всіх послугах, яку зобов'язаний зареєструвати (опублікувати) в ньому провайдер відповідної послуги. Споживач сервісу відправляє необхідний запит в реєстр, який і забезпечує скріплення його з провайдером.

На рис. 7.14 представлені три основні операції, передбачені архітектурою SOA. Постачальник послуги опубліковує інформацію про свої служби в реєстрі служб, де їх знаходить споживач служб. Використовуючи знайдену інформацію, він зв'язується з послугою (викликає її, ініціює взаємодію з нею).

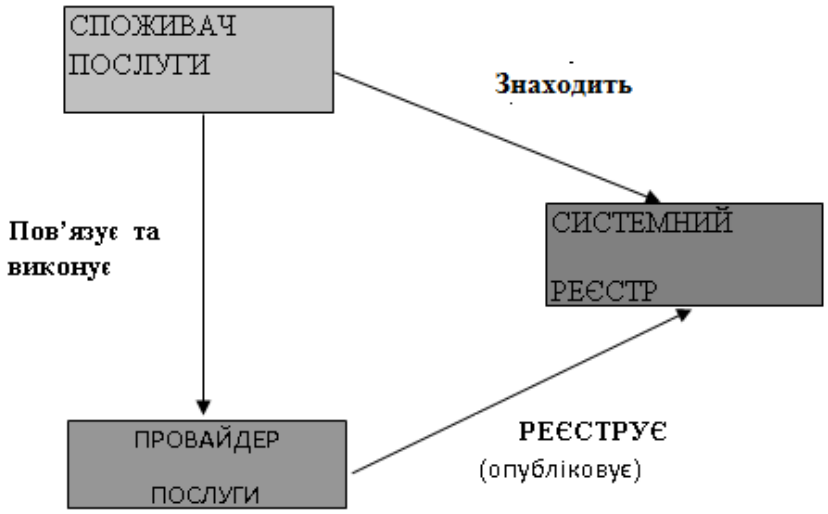


Рис. 7.14. Парадигма “знайти, зв’язати і виконати”

Для створення SOA необхідні два основних типу угод між провайдером і споживачем послуги:

- за транспортним механізмом, що визначає формати і протоколи;
- за форматами повідомлень і типами даних.

Система управління телекомунікаційною мережею направляє і контролює послугу протягом її життєвого циклу - від установки і конфігурації до виконання з урахуванням конкретних вимог.

Сервіс-орієнтовна архітектура, підтримуючи зміни в моделі ведення бізнесу, будується так, щоб ізолювати вплив модифікації одного компоненту на решту частини середовища.

Рішення на базі сервіс-орієнтовної архітектури дозволяють використовувати переваги розподілених послуг і забезпечують взаємодію процесів бізнесу, дозволяючи оптимізувати процес управління мережею.

Рівень управління послугами може включати безліч незалежних підсистем ("мереж послуг"), що базуються на різних технологіях, що мають своїх абонентів і що використовують свої, внутрішні системи адресації.

Операторам зв'язку потрібні механізми, що дозволяють швидко і гнучко розгортати, а також змінювати послуги залежно від індивідуальних потреб користувачів.

На даному етапі свого розвитку сервіс-орієнтовні архітектури для опису і організації взаємодії використовують базові стандарти Web-сервісів:

- eXtensible Markup Language (XML) — для представлення даних;
- Web Services Definition Language (WSDL) — для опису доступних Web-сервисов;
- Universal Description, Discovery, Integration (UDDI) — для створення каталога доступних по мережі Web-сервисов;
- Simple Object Access Protocol (SOAP) — для обміну даними.

Таким чином, сервіс-орієнтовна архітектура заснована на принципі прозорої взаємодії різнорідних програмних компонентів (сервісів) і побудови на їх основі автоматизованих процесів бізнесу.

Як правило, організація телекомунікаційної послуги передбачає наступні стадії (кожна з яких сама по собі досить складний бізнес-процес):

- маркетингове просування послуги;
- обробка запиту клієнта;
- оцінка технічної можливості організації послуги;
- укладення договору з клієнтом;
- виконання роботи по організації послуги;
- технічна експлуатація; контроль якості;
- білінг; контроль балансу і виставляння рахунків;
- управління дебіторською заборгованістю клієнтів;
- управлінський і бухгалтерський облік операцій.

Бізнес - процеси управління мережею описуються в рекомендаціях ITU-T серії М.3050.х. процеси Бізнесу представлені у вигляді багаторівневої матриці, званою розширеною схемою телекомунікаційних операцій (eTOM).

При створенні автоматизованої системи управління діяльністю оператора (провайдера) необхідно вирішити такі завдання:

- проаналізувати процеси eTOM, щоб визначити набір елементів бізнес - логіки, що визначає модель;
- виділити і специфікувати елементи бізнес - логіки, забезпечивши тим самим можливість конфігурації з набору будь-якого бізнес - процесу в майбутньому;
- розробити специфікацію, засновану на існуючих стандартах підприємства замовника і відповідну набору елементів (фактично що включає їх);
- утілити елементи бізнес - логіки в програмний код.

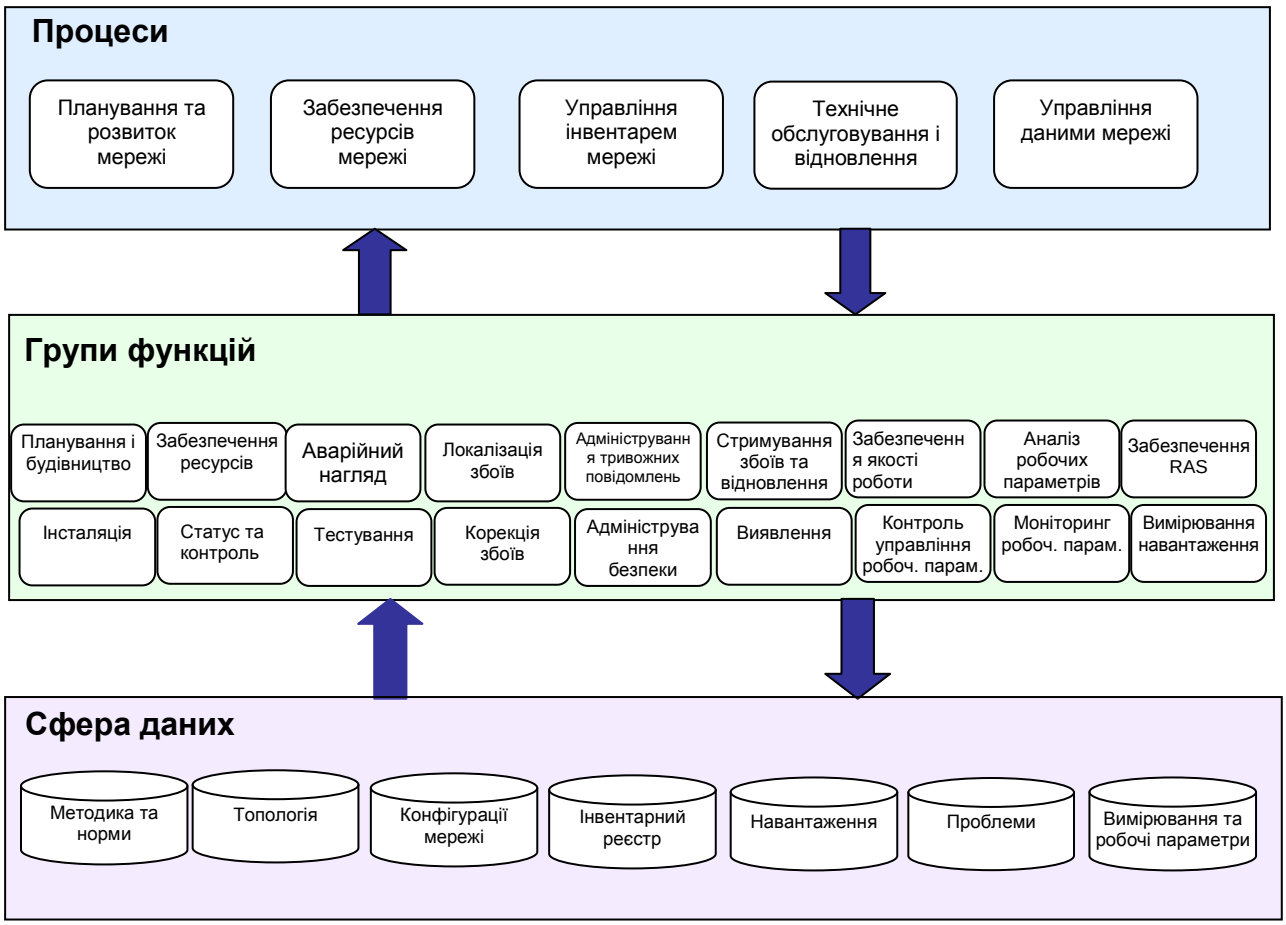
Можна виділити горизонтальні і вертикальні потоки процесів. Модель, описана eTOM і представлена на рис. 7.15, застосовується і для управління NGN. Модель eTOM відображає структуру бізнес-процесів, необхідних провайдеру послуг.

Рис. 7.15. Модель eTOM – 1-й рівень декомпозиції

Таким чином, розглядаючи проекцію функціональної моделі управління на загальну архітектуру управління мережами NGN, можна відзначити, що функціональна модель може розглядатися за допомогою двох методів:

Розглядаючи проекцію функціональної моделі управління на загальну архітектуру управління мережами NGN, необхідно відзначити, що функціональна модель може розглядатися за допомогою двох методів:

- Метод функція/послуга управління, описаний в M.3200 і M.3400, який був побудований на вимогах, що пред'являються до керованого мережного обладнання і мереж (від низу до верху);
- Метод бізнес-процеса, описаний в M.3050.x (eTOM), який був побудований на необхідності підтримувати процеси всього підприємства провайдера послуг (зверху вниз).



Примітка. RAS (reliability, availability, serviceability) – Надійність, доступність, зручність в обслуговуванні

Рис. 7.16.Процеси, групи функцій і області даних

З часом, обидва підходи об'єднаються в єдиний метод бізнес-процесу, при якому послуги управління розглядатимуться як частини бізнес-процесів. Перший крок в цьому напрямі, це початкове відображення M.3400 в M.3050.x і навпаки, встановлене в M.3050/ Suppl.3, яке перетворить метод «бізнес-

процесу» в метод «функції управління/бізнес-процесом». Взаємозв'язок між процесами 2-го рівня декомпозиції згідно моделі eTOM з відповідними їм наборами функцій і сферами даннях представлений на рис.7.16.

Для того, щоб спростити уявлення про управління NGN, функціональність управління може бути розбита на логічні рівні або функціональні рівні управління. Логічна рівнева архітектура (LLA) це принцип побудови функцій управління, при якому функції групуються в так звані «логічні рівні» і описуються стосунками між рівнями. Логічний рівень відображає певні аспекти управління, організованого різними рівнями абстракції. Логічна рівнева архітектура управління NGN показана на рис. 7.17.

Як видно з рисунку функціональні блоки управління згруповані в логічні рівні. Спеціалізація OSFs, заснованих на різних рівнях абстракції, наступна:

- Управління підприємством;
- Управління ринком, продуктом і замовником;
- Управління послугами NGN;
- Управління ресурсами;
- Управління елементом послуги і транспорту;
- Управління взаєминами між постачальниками і партнерами.

Для зв'язку між функціональними блоками служать еталонні (контрольні) точки, які в архітектурі MNGN (управління NGN) належать до одного з трьох класів:

- точки класу q – розташовуються між блоками OSF або NEF. У цій точці надаються функції управління, які вимагає інший OSF або NEF або споживаються функції управління, які надають інші блоки OSF або NEF.
- точки класу b2b/c2b – еталонна точка, що надається з боку OSF одного адміністративного домена для використання OSF в іншому адміністративному домені В термінах TMN відповідають інтерфейсу X.
- точки класу hmi – еталонна точка, що надається для використання фізичним користувачем.

Еталонна точка, в якій надається деяка функціональність, що виробляється функціональним блоком, називається еталонною (контрольною) точкою провайдера і на рисунку відображується заповненим кружечком. Відповідно, еталонна точка, в якій споживається деяка функціональність, називається еталонною точкою споживача і на рисунку відображується напівмісяцем.

Таким чином, особливості управління NGN визначаються особливостями архітектури мережі NGN, а саме:

1.Організація з'єднання в NGN має принципові відмінності від його встановлення в традиційних телефонних мережах з комутацією каналів. Це пов'язано з тим, що медіатрафік і сигнальна інформація для управління обслуговуванням виклику в NGN передаються по різних маршрутах і обробляються різними мережними пристроями, а не єдиним вузлом комутації.

2. Медіатрафік проходить, як правило, безпосередньо між шлюзами доступу (наприклад, мультисервісними абонентськими концентраторами - МАК) або транспортними шлюзами. Сигналізація управління обслуговуванням виклику проходить через програмні комутатори Softswitch, а в простіших випадках – через проксі-сервери SIP або гейткипери H.323, але завжди не там, де медіашлюзи і медіатрафік.

3. При наданні послуги сеансового доступу користувача до мережі IP вузол мережі, що відповідає за ідентифікацію користувача, не бере участь в передачі користувачевої інформації і, як наслідок – неможливість отримання користувачевої інформації для єдиного пристрою управління, що визначає параметри з'єднання по номерах викликаючого користувача або користувача, що викликається.

Вимогами, що пред'являються до систем управління NGN, є:

1. Необхідність розподілу функцій управління в декількох мережних пристроях, у тому числі:

- у пристрої управління викликами і сеансами зв'язку (Softswitch, гейткипер, SIP-проксі);
- у пристрої мережі, що відповідає за перенесення користувачевої інформації.

2. Впровадження відкритих інтерфейсів управління, що дозволяють управляти різнотипним обладнанням (включаючи мережні вузли, міжмережні шлюзи і ін.), яке входить до складу NGN, у тому числі, використання стандартизованих протоколів - IIOP, CMIP, SNMP, TFTP, FTAM і формальних мов для опису інтерфейсів – CORBA IDL, JAVA, GDMO).

3. Структура систем управління NGN повинна забезпечувати гнучкість реалізації і сумісність з іншими рішеннями, високу надійність, і як результат – якість обслуговування;

4. Оператор повинен мати можливість модифікувати програмне забезпечення для реалізації специфічних функцій і вводити нові послуги через зміну конфігурації:

- компонентні рішення спростять можливості оператора по введенню нових користувачів і функцій;

- гнучкість і масштабованість дозволять легко адаптуватися до нових технологій, що швидко з'являються, і продуктів, а також до потреб користувачів, що змінюються.

5. Вищевикладеним вимогам відповідає архітектура eTOM, запропонована TM Forum. Практична реалізація бізнес-процесів і взаємодії між ними повинна відповідати вирішенням орієнтованої для сервісу архітектури SOA.

6. З подальшою еволюцією NGN з великою часткою вірогідності можна передбачити, що процес управління розглядатиметься не по відношенню до одного окремо взятого оператора або сервіс-провайдера, а до співтовариства таких операторів і сервіс-провайдерів, що беруть участь в наданні послуги кінцевому споживачеві (Supply Chain). Лише при такому розумінні можна побудувати наскрізні (end-to-end) і безшовні (seamless) процеси надання послуг, підтримувані в розподіленому (між учасниками процесу) управляючому середовищі платформ і систем. В термінах моделі eTOM це означає, що процеси рівня управління послугами в значній мірі визначатимуться рівнем управління взаємодією з партнерами і постачальниками (Supply/Partnership Management).

7.4 Методологія NGOSS

Основою, що забезпечує роботу ефективного оператора, є високоефективний механізм бізнесу, орієнтований на вдосконалення бізнес - процесу, тобто, на збільшення гнучкості і прудкості реакції бізнесу, скорочення операційних витрат і підвищення якості обслуговування клієнтів. Три основні компоненти складають основу ефективного оператора телекомунікацій. Ці компоненти представлені на рис.7.18.

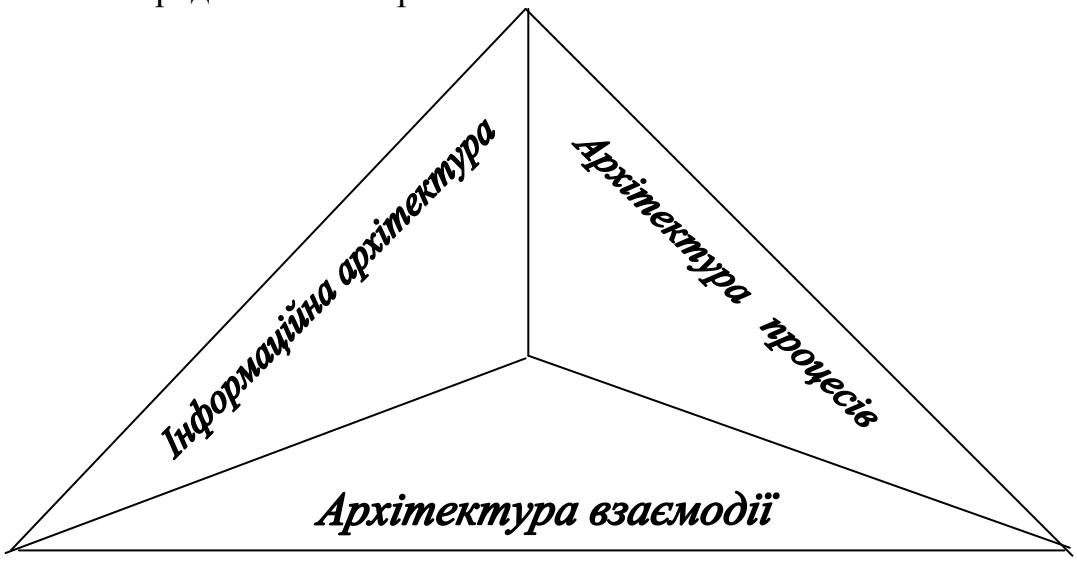


Рис. 7.18. Базова архітектура ефективного оператора

Інформаційна компонента забезпечує співробітників підприємства будь-якою необхідною інформацією в режимі реального часу (“on-line”). Реалізується вона за допомогою автоматизованих систем (систем управління базами даних і базами знань), що дозволяють зручний інтерактивний режим роботи з ними і, що забезпечує своєчасне і регулярне оновлення інформації, що зберігається.

Друга компонента, звана архітектурою процесів, реалізує стратегії і тактики оператора телекомунікацій для досягнення поставлених цілей. Архітектура процесів задає структуру, що визначає організацію процесів і їх адаптацію до змін в галузі.

Архітектура взаємодії формалізує інтерфейси між архітектурою процесів і інформаційною архітектурою, визначаючи тим самим інформацію, необхідну для виконання процесу; інформацію, що отримується в результаті виконання процесу.

Як спеціалізований інструмент, за допомогою якого ефективний оператор телекомунікацій розробляє і упроваджує проекти автоматизації, TM Forum запропонував використовувати структуру, звану NGOSS (New Generation Operations Systems and Software – Операційні системи і ПО нового покоління). Фактично NGOSS є набором інструментів, що складається з керівних принципів і специфікацій, що погоджених в рамках галузі і охоплюють ключові зони бізнесу і технології. У узагальненій формі NGOSS складається з чотирьох структур, представлених на рис.7.19.

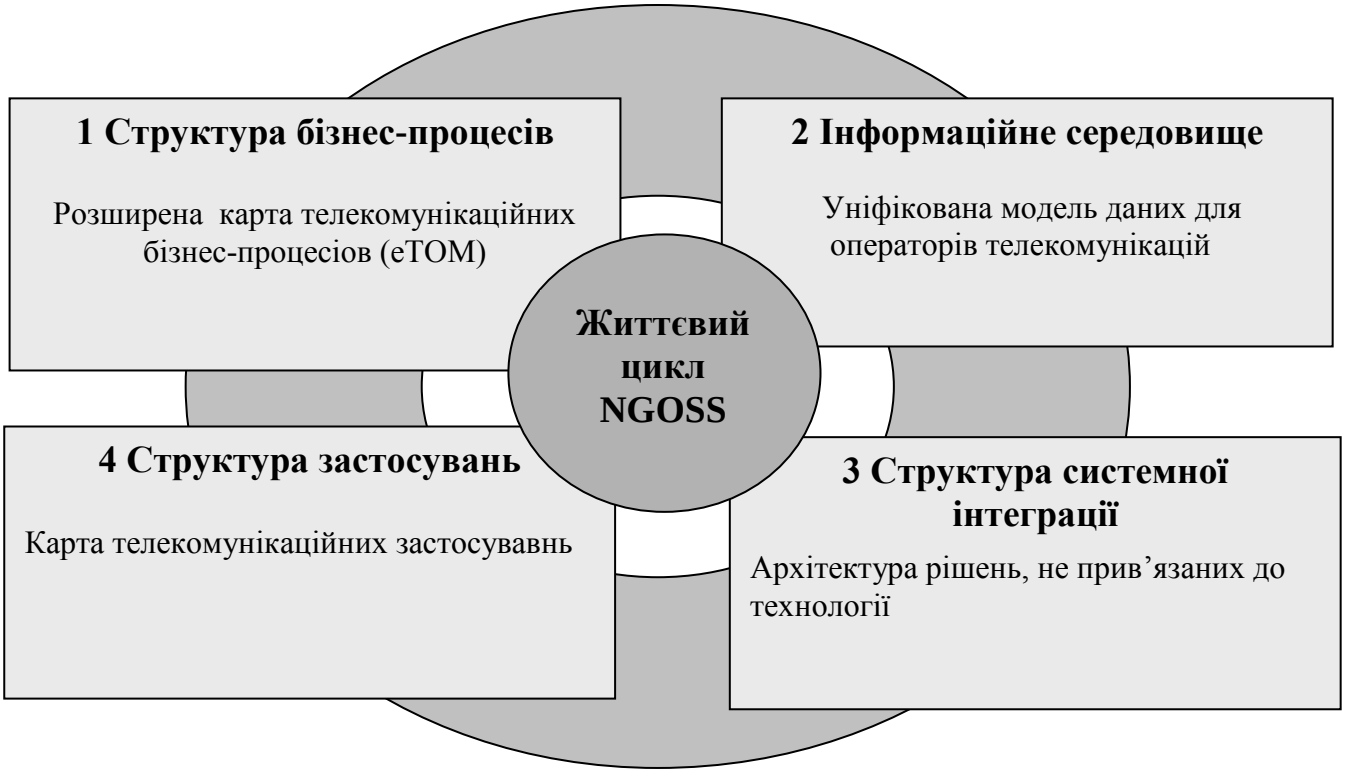


Рис. 7.19. Структура NGOSS

Перша складова (рис.7.19) – це структура бізнес - процесів, яка описується за допомогою розширеної карти телекомунікаційних операцій eTOM (enhanced Telecom Operations Map). Можна сказати, що eTOM є еталонною структурою, яка класифікує по категоріях всі типі бізнес - діяльності оператора телекомунікацій і створює, тим самим, умови для формування крізних бізнес - процесів (наприклад, процес надання послуги). Карта eTOM забезпечує структурну декомпозицію процесів, послідовно уточнюючи їх у міру підвищення рівня деталізації. Спочатку карта eTOM передбачає розділення між стратегічними процесами, операційними процесами і процесами управління підприємством. Ці три групи процесів є процесами нульового рівня. На рисунку 7.15 представлена карта eTOM – декомпозиція процесів рівня 1. На рисунку показано яким чином співвідносяться процеси нульового і першого рівнів декомпозиції. Виділено сім вертикальних потоків процесів. Операційна діяльність передбачає наявність чотирьох вертикальних потоків процесів, причому, перший з них – забезпечення готовності і операційна підтримка – забезпечує створення експлуатаційного середовища, в якому реалізуються останні потоки процесів. Ці потоки (другий, третій і четвертий) орієнтовані на роботу з клієнтом в реальному масштабі часу і відповідають за реалізацію послуги, забезпечення якості і білінг. Саме тому ці процеси необхідно автоматизувати в першу чергу.

Процес нульового рівня «стратегія, інфраструктура і продукт» розбитий на три вертикальні потоки процесів. Ці процеси не приймають безпосередньої участі в роботі з клієнтом. Потік процесів «стратегія розвитку» пов'язаний із створенням інфраструктури телекомунікацій. Процеси потоків «управління життєвим циклом інфраструктури» і «управління життєвим циклом продукту» відповідають за стратегічне планування розвитку оператора телекомунікацій.

Системи, що підтримують операційні процеси моделі eTOM називають OSS-системами (Operations Support System), а системи, що підтримують процеси стратегії, інфраструктури і продукту моделі eTOM, – BSS-системами (Business Support System). Необхідно відзначити, що існують деякі розбіжності при вживанні цієї термінології. Якщо поглянути на карту eTOM (рис.7.15, то можна відмітити, що згідно визначенню, до систем BSS можна віднести системи аналізу і прогнозування бізнесу (Business Intelligence), систему CRM (у частині автоматизації процесів маркетингу), аналітичні модулі (системи знань) і автоматизовані системи підтримки збалансованих показників (BSC) діяльності оператора телекомунікацій. Системи управління мережами і мережними елементами, взаємодії з клієнтами, білінг, системи управління замовленнями, інвентаризації, захисту від шахрайства, управління якістю обслуговування SLA відносяться до систем OSS.

Проте, часто системи, що забезпечують управління взаєминами з клієнтами, партнерами, також як і биллинг відносять до систем BSS. Не існує

однозначного тлумачення цих понять. Тому на сьогоднішній день актуальною стає розробка вітчизняних нормативних документів, що регламентують опис термінів і визначень, впрваджених в моделі eTOM.

Ефективність функціонування оператора телекомунікацій безпосередньо залежить від того, яким чином він моделював свої бізнес-процеси. Особливе значення набуває моделювання наскрізних бізнес-процесів. Усередині організації практично завжди існують проблеми міжфункціональної взаємодії підрозділів, які призводять до зниження ефективності діяльності організації в цілому.

Для забезпечення адекватного управління на міжфункціональному рівні, необхідно використовувати наскрізні бізнес-процеси. Як приклади наскрізних процесів можна привести процеси управління замовленням (Order Management), обробки і вирішення проблем (Help Desk/Service Desk/Trouble Ticketing), врегулювання претензій щодо білінгу (Billing Disputes and Adjustments), розробка і впровадження на ринок нових продуктів.

Проте, перш ніж ставити питання про впровадження нових систем необхідно провести опис і при необхідності реінжиніринг процесів. Це передбачає аналіз існуючого положення справ («як є») і вироблення рекомендацій по раціональній організації процесів («як повинно бути»). При цьому визначаються учасники процесів, їх функції, порядок їх взаємодії.

Друга складова (рис.7.19) – це уніфікована інформаційна модель SID (Shared Information/Data Model), яка доповнює eTOM, і є еталонною моделлю даних, що забезпечує єдину мову опису об'єктів управління, що, у свою чергу полегшує процес інтеграції програмних застосувань для системи підтримки операційної і бізнес-діяльності операторів (OSS/BSS) від різних постачальників. Ця модель зв'язує розподілену і різнорідну інформацію в єдину структуру, що управляє, дозволяє контролювати вирішення розподілених проблем. Крім того, будучи глобальною моделлю, вона дозволяє здійснювати доступ до даних, у тому числі, до інформаційних баз галузевих асоціацій, органів стандартизації і компаній – членів TM Forum [28].

Інформаційна модель підприємства базується на концепції уніфікованості даних для однотипних процесів різних операторів телекомунікацій. Ця модель може поетапно деталізувати на детальніші інформаційні структури подібно до того, як карта eTOM відображує рівні декомпозиції для процесів. Так першому рівню декомпозиції карти eTOM відповідає інформаційна структура, звана доменом. Другому рівню декомпозиції згідно карти eTOM відповідає інформаційна структура, звана агрегованою бізнес - сутністю. Агрегована бізнес-сутність – це набір даних і операцій, що характеризують стійку сукупність бізнес - сутностей. Таким чином, домен – набір агрегованих бізнес - сутностей, відповідних деякій зоні управління.

Бізнес-сутності – це найнижчий рівень декомпозиції в рамках моделі SID, тобто, бізнес-сутність є деякою елементарною інформаційною структурою, за допомогою якої можна описати бізнес-модель. В якості мови опису моделі використовується універсальна мова моделювання UML. Існує множина моделей SID, запропонованих організаціями – членами TM Forum.

Переваги використання єдиної інформаційної моделі полягають у наступному:

– створюється єдиний формат збору та обміну даними як в рамках одного підприємства, так і між різними підприємствами;

– істотно спрощується задача інтеграції різних модулів систем управління підприємством;

– можливість ведення єдиної бази даних для всіх бізнес-процесів дозволяє передавати контроль над бізнес-процесом від одного модуля до іншого, що забезпечує його цілісність і наскрізне виконання;

– забезпечуються умови для впровадження і ведення корпоративних каталогів продуктів, послуг і ресурсів, що дозволяє одержати повні об’єктивні відомості для аналізу ефективності використання ресурсів, оптимальності вибудуваної системи продажів, привабливості запропонованої продукції та ін.

Етапи аналізу даних за допомогою SID тісно пов’язані з життєвим циклом NGOSS і включають три його ракурси: бізнес-ракурс, системний та ракурс впровадження. У першому випадку завдання аналітика полягає у виділенні інформаційних елементів, задіяних в бізнес-процесах компанії та визначенні їх найважливіших властивостей. Аналіз даних з точки зору системи орієнтований, перш за все, на вивчення особливостей взаємодії елементів даних і операцій, які можна здійснювати з тим чи іншим елементом. На рівні впровадження на перший план виходять питання, пов’язані з практичним втіленням розробленої інформаційної моделі.

Модель SID складається з трьох основних частин:

а) системна інформаційна карта (англ. Systems and Information Map –SIM), що структурує елементи даних;

б) опис інформаційних сутностей та їх атрибутів;

в) графічні діаграми для кожної бізнес-сутності в нотації UML.

Системна інформаційна карта розроблена для структурування даних, що складають модель SID. Основним структурним елементом карти SIM є інформаційна сутність – одиниця даних, яка має набір даних, що описують її атрибути та бере участь у відносинах з іншими сутностями. Сутністю може бути матеріальний об’єкт, вид діяльності або поняття. Сутності в карті розбиті по доменах відповідно до характеру інформації, яку вони описують, що визначає рівневу структуру моделі SID. Як і бізнес-процеси, інформаційні сутності

підлягають деталізації. Кожен домен є відносно замкнутим, елементи всередині нього сильно пов’язані між собою.

Системна інформаційна карта тісно пов’язана з картою eTOM. Її структура відповідає групам процесів eTOM, також збережений принцип аналізу досліджуваних об’єктів, що полягає у їх послідовній декомпозиції. Співвіднесення кожного домена з деякою групою бізнес-процесів карти eTOM спрощує аналіз інформаційних потоків, пов’язаних з діяльністю компанії, і дозволяє виділити найбільш важливі для вирішення того чиїншого завдання складові.

Для опису кожної інформаційної сутності в SID використовуються дві таблиці. У одній із них наводиться текстовий опис сутності, перераховуються моделі, в яких вона також визначена, а крім того, зазначені класи, з якими сутність взаємодіє. Крім цього, у даній таблиці передбачено поле для опису правил використання та реалізації сутності. Інша ж таблиця характеризує атрибути сутності. У неї включають назву та опис атрибутів, тип даних, ознаки обов’язковості або необов’язковості атрибутів, особливості використання та зауваження, що вказуються в довільній формі.

Для графічного опису відносин між сутностями і специфіки їх взаємодії застосовується нотація UML, що уніфікованим і наочним чином відображає особливості використання тієї чи іншої інформації. Це, по-перше, сприяє досягненню порозуміння між сторонами, що працюють з інформаційною моделлю протягом усього її життєвого циклу, а по-друге, дозволяє скористатися всіма можливостями такої потужної та ефективної мови моделювання, як UML.

Третя складова (рис.7.19) - структура системної інтеграції - є, технологічно нейтральна архітектура TNA (Technology Neutral Architecture), що визначає основні принципи розробки рішень на базі NGOSS. Термін «технологічно нейтральна» означає незалежність архітектури від технології впровадження, яка буде реалізована в NGOSS, тобто ця архітектура описує не конкретну реалізацію, а принципи, які повинні використовуватися при розробці рішень на базі NGOSS.

TNA охоплює різноманітні архітектурні проблеми, включаючи, зокрема, загальні інтерфейси між компонентами (так звані контрактні інтерфейси), структури розподілу, загальні механізми комунікацій і керування стратегією і процесами. Ця архітектура є ключовим інструментом NGOSS в побудові OSS рішень в незалежному від технологій (бази даних, мова програмування та ін.), що застосовуються, вигляді. Даний інструмент призначений для користування розробниками OSS систем. Його використання при проектуванні системи означає дотримання однакового стилю розробки, що забезпечує високі

показники надійності програмного забезпечення, мінімізацію трудовитрат і потенційну готовність до інтеграції з іншими системами, що теж використовують цей стиль.

Незалежність від технологій реалізації дозволяє використовувати дану архітектуру будь-якому розробнику, незалежно від того, на базі яких серверів, застосувань, баз даних, мов програмування побудована OSS система. За рахунок використання TNA досягаються:

– високі показники повторного використання програмного коду (мінімізація дубльованого програмного коду);

– високі характеристики коректності та стійкості до помилок коду програмного забезпечення;

– підвищується здатність системи до інтеграції з іншими TNA-сумісними системами.

Четверта складова (рис.7.19) – структура застосувань (карта застосувань) TAM (Telecom Applications Map) – забезпечує представлення структури програмних застосувань і дозволяє відображувати складові частини процесів на конкретні застосування незалежних розробників.

Будучи одним з інструментів NGOSS, карта TAM містить класифікацію функцій застосувань та інформаційних систем, що автоматизують діяльність інфокомунікаційної компанії, і забезпечує мову і основу для спілкування постачальників рішень OSS/BSS з їх користувачами. Оператори зв’язку можуть застосовувати карту TAM для опису наявної інфраструктури ПЗ або формулювання вимог до застосувань і набору модулів, а виробники – для опису можливостей наданих ними систем.

TAM була розроблена, як робочий посібник, що допомагає операторам зв’язку використовувати загальну довідкову Карту та мову для переміщень по складному системному ландшафту, у якому зазвичай функціонують оператори фіксованого, мобільного та кабельного зв’язку. Там, де eTOM забезпечує представлення структури телекомунікаційних бізнес-процесів, карта TAM забезпечує представлення структури програмних застосувань. TAM використовується на ранніх стадіях розробки в межах TM Forum.

NGOSS визначає новий підхід до процесу розробки та використання систем управління. Цей підхід ґрунтується на понятті життєвого циклу NGOSS, що докладно описує етапи розробки рішення і завдання розробника, пов’язані з кожним з них. Засобами для вирішення цих завдань служать компоненти NGOSS.

На додаток до основних структурних елементів NGOSS визначає також

ітеративну методологію життєвого циклу розробки, що зазвичай має назву SANRR (Scope (визначення кордонів), Analyse (аналіз), Normalize (нормалізація), Rationalise (раціоналізація), Rectify (коректування)).

Життєвий цикл NGOSS та методологія SANRR забезпечують загальну структуру, що описує порядок використання та розгортання NGOSS в межах організації. Розробка проходить через чотири ракурси NGOSS у рамках послідовного ітеративного процесу.

Життєвий цикл NGOSS включає п'ять послідовно виконуваних етапів (ітерацій) (рис.7.20):

- Визначення границь рішення, виходячи з комерційної мети рішення, включаючи цілі і бізнес - сценарії високого рівня;
- Аналіз бізнес - середовища для рішення, що розробляється, - включає підготовку документації по бізнес - процесам, інформації і політиці;
- Нормалізація взаємодії всіх компонентів за допомогою уніфікованої інформаційної моделі;
- Раціоналізація бізнес – процесів - включає ідентифікацію нових процесів і політик, визначення функціональних можливостей і технологій, необхідних для виконання поставлених цілей (досліджується нормалізована модель на предмет необхідних змін - розриви, повтори, конфлікти);
- Корегування бізнес - процесів – включає впровадження нових процесів і політик, функціональних можливостей і технологій, визначених на етапі раціоналізації, а також модифікацію існуючих процесів, політик і функціональних можливостей.

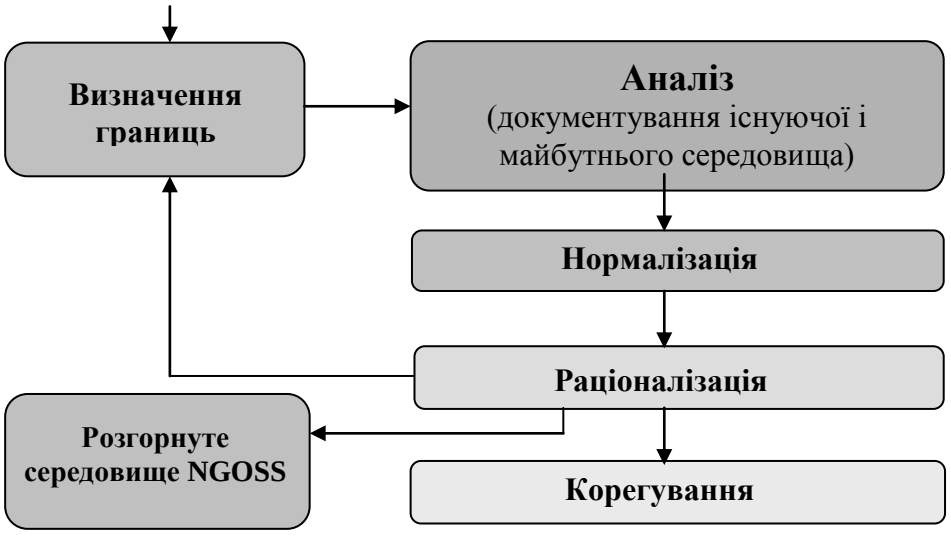


Рисунок 7.20. Ітерації життєвого циклу NGOSS

Крім того життєвий цикл NGOSS має чотири форми вистави (ракурсу), а саме (рис.7.21):

- бізнес;
- система;
- впровадження;
- розгортання.

Бізнес-ракурс відображає бізнес-процеси, інформаційну модель і їх взаємодію. Тобто, опис бізнес-процеса і відповідних йому доменів і бізнес-сутностей забезпечує бізнес-ракурс.

Системний ракурс розширює бізнес-ракурс шляхом введення таких понять як контракти, сценарії і бізнес-сутності, за допомогою яких виконується деталізований опис взаємодії між різними елементами інформаційної і бізнес-структур. Наприклад, додається операція «отримати дані про всі фізичні порти» або «результати тестування карти» і так далі.

Сценарії і контракти є тим інструментом, за допомогою якого описується взаємодія між інформаційною моделлю SID і процесами eTOM.

Ракурс впровадження відображає створення програмних і апаратно-програмних засобів, необхідних для досягнення поставленої мети без прив'язки до конкретної технології, визначаючи тим самим технологічно нейтральне рішення для поставленої мети.

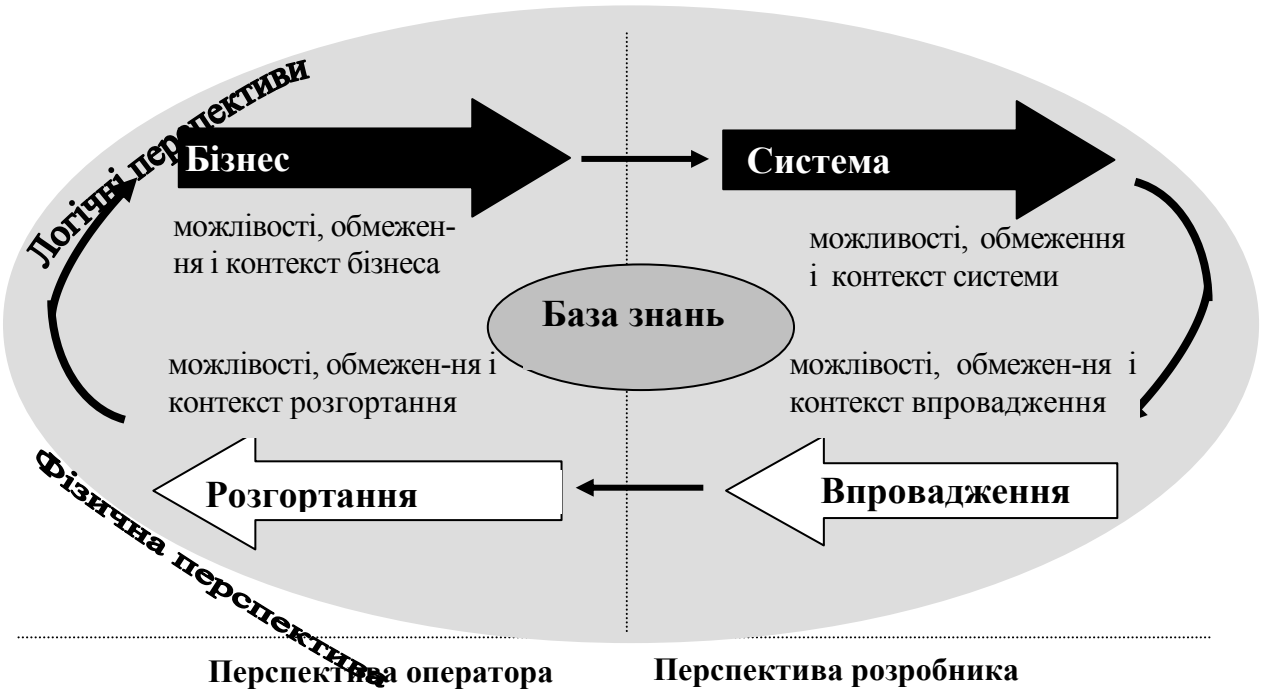


Рисунок 7.21. Формы представлення (ракурси) життєвого циклу NGOSS

Ракурс розгортання відображує експлуатацію і моніторинг вибраних інструментів для досягнення мети, у тому числі, перенесення застосування з одного середовища в іншу без внесення змін до інших форм вистави.

Логічна і фізична персперктивы позволют відокремити технологічно нейтральні ракурси (бізнес-ракурс, системний ракурс) від технологічно залежних ракурсів впровадження і розгортання.

Перспективи оператора телекомунікацій і розробника послуг перетинаються з логічною і фізичною перспективами. Перспектива оператора телекомунікацій у межах логічної перспективи представляє рішення NGOSS в термінах, прийнятих і зрозумілих операторові телекомунікацій. А перспектива оператора телекомунікацій у межах фізичної перспективи представляє робоче застосування, яке використовується для реалізації бізнес-процесів оператора телекомунікацій. Перспектива розробника послуг телекомунікацій у межах логічної перспективи представляє рішення NGOSS в термінах, які розробник використовує при створенні рішення. Перспектива розробника послуг у межах фізичної перспективи пов'язана з технологіями, які розробник використовує при створенні рішення.

Необхідно відзначити, що NGOSS не є рішенням, яке необхідно упроваджувати відразу і повністю. Переважно поетапне впровадження NGOSS. Наприклад, підприємство може упровадити модель уніфікованого інформаційного середовища SID, а потім, поетапно розвертати карту процесів і карту застосувань згідно цієї моделі.

Першим кроком впровадження карти процесів є аналіз процесів, що діють на підприємстві, і проектування їх на eTOM. Наприклад, можуть бути виділені такі ключові процеси:

- управління якістю обслуговування;
- управління замовленнями;
- управління при відмовах;
- підключення і активація послуги;
- управління продуктивністю;
- управління конфігурацією;
- білінг;
- інвентаризація послуг і ресурсів.

Другим кроком впровадження карти процесів є проектування виділених процесів на карту eTOM другого рівня декомпозиції, тобто на цьому етапі впровадження визначається яким чином співвідносяться виділені процеси з процесами, стандартизованными картою eTOM. Таким чином, виявляються процеси, які не були враховані розробником, але присутні на карті (взаємини з постачальниками і партнерами), процеси, які недостатньо деталізовані (біллінг, процеси управління при відмовах, управління продуктивністю) і процеси, які

відносяться до одного і того ж процесу рівня 2 (збір даних про завантаження ресурсів).

Третім кроком впровадження карти процесів є подальша деталізація проекції процесів на карту eTOM третього рівня і створення таблиці відповідності між реальними процесами оператора телекомунікацій і формалізованими процесами eTOM.

Таким чином, резюмуючи вищевикладене, можна сказати, що концепція NGOSS є набором стандартизованных специфікацій і керівництва, яке охоплює найважливіші області діяльності оператора телекомунікацій:

- стандартну архітектуру бізнес-процесів оператора телекомунікацій, що дозволяє всім зацікавленим сторонам в області телекомунікацій розуміти один одного;
- стандартний опис інформації управління, що дозволяє об'єктам управління взаємодіяти один з одним;
- опис вимог і принципів побудови систем управління, що реалізовують стандартні бізнес-процеси і що використовують стандартний опис інформації з максимальним використанням готового інтегрованого програмного забезпечення, компоненти якого, можна додавати, видаляти або модифікувати за принципом простої установки (Plug and Play).

Впровадження концепції NGOSS і моделі eTOM в діяльність оператора телекомунікацій забезпечить:

- створення універсальної інтегрованої структури для розробки, виробництва, розгортання систем і програмного забезпечення для систем підтримки експлуатації і бізнесу;
- взаємодію операторів телекомунікацій між собою на рівні стандартних бізнес-процесів, що у свою чергу дозволить надавати наскрізні послуги клієнтам, розвивати найбільш прогресивні бізнес-моделі;
- широке використання інформаційних систем операторами телекомунікацій для автоматизації процесів з меншими витратами, чим при використанні нестандартних підходів;
- відсутність залежності оператора телекомунікацій від вирішень одного постачальника інформаційних систем (мультивендорность);
- сумісність інформаційних систем різних постачальників.

Перспектива оператора зв’язку та розробника послуг проникає через межі відповідних ракурсів до іншої перспективи. Інтерес постачальника послуг у бізнес-ракурсі в рамках логічної перспективи пов’язаний з формулюванням рішення у зрозумілих йому термінах. Інтерес оператора у ракурсі розгортання в рамках фізичної перспективи пов’язаний з робочим застосуванням, який використовується для реалізації бізнес-процесів у оператора. Інтерес розробника

послуг у системному ракурсі в рамках логічної перспективи виражається у термінах, які розробник використовує при створенні рішення; інтерес розробника послуг у ракурсі реалізації в рамках фізичної перспективи пов'язаний із технологіями, які він використовує при реалізації рішення.

Сервісна орієнтація NGOSS відділяє специфікації рішень від технологій виконання. Можливості рішення надаються користувачеві у вигляді сукупності компонентів, пов'язаних за допомогою механізму, що повністю описує взаємодію між компонентами. Сервіс-орієнтована архітектура також забезпечує механізм для ідентифікації та локалізації сервісів, що реалізуються через контрактні обов'язки між користувачами та компонентами – постачальниками сервісів.

Використання життєвого циклу розробки NGOSS забезпечує ряд дуже важливих стратегічних переваг, з його допомогою можна інтегрувати до єдиної архітектури бізнес вимоги та технічні аспекти діяльності оператора зв'язку, автоматизувати бізнес-процеси в гетерогенних IT-середовищах, побудувати єдину інформаційну інфраструктуру, орієнтовану на виконання бізнес-завдань інфокомунікаційної компанії.

Контрольні питання

1. Визначте основні функції Softswitch.
2. Яке призначення транспортної площини в архітектурі Softswitch?
3. Назвати протоколи взаємодії Softswitch з іншим обладнанням NGN.
4. Пояснити, що таке SIP-адрес. Наведить можливі формати SIP-адресів.
5. Пояснити основне призначення концепції IP Multimedia Subsystem.
6. Яке призначення функції управління сеансом зв'язку згідно архітектури IMS?
7. Сформулюйте призначення обслуговуюча функція S-CSCF в архітектурі IMS.
8. Сформулюйте призначення серверу абонентів домашньої мережі HSS.
9. Назвати варіанти реалізації білінга згідно архітектури IMS.
10. Сформулюйте призначення і формати ідентифікатора PrUI.
11. Провести порівняльну характеристику Softswitch і IMS.
12. Визначте архітектуру управління NGN.

13. Пояснити призначення сервіс-орієнтовної архітектури.
14. Назвати компоненти сервіс-орієнтовної архітектури.
15. Визначте основні горизонтальні і вертикальні потоки процесів моделі eTOM.
16. Сформулюйте призначення еталонних точок в логічної архітектурі управління NGN.
17. Назвати базові компоненти моделі управління за методологією NGOSS.
18. Сформулюйте призначення інформаційної моделі SID.
19. Що таке бізнес-сутність в моделі SID ?
20. Визначте етапи впровадження NGOSS.

Література

1. Амато, Вито.Основы организации сетей Cisco, том 1. : Пер. с англ. - М. : Издательский - дом "Вильяме", 2002. - 512 с.
2. Амато, Вито.Основы организации сетей Cisco, том 2. : Пер. с англ. - М. : Издательский - дом "Вильяме", 2002. - 464 с.
3. Анкудинов Г.И., Стрижаченко А.И. Сети ЭВМ и телекоммуникации. Архитектура и протоколы: Учеб.пособие. – СПб.: СЗТУ, 2001. – 92 с.
4. Бакланов И.Г. NGN:принципы построения и организации. – М.: Эко-Трендз, 2008. – 400 с.
5. Битнер В.И. , Михайлова Ц.Ц. Сети нового поколения. . – Горячая Линия - Телеком, 2011 г. – 226 с.
6. Блэк Ю. Сети ЭВМ: протоколы, стандарты, интерфейсы. – М.: Мир, 1990. – 506 с.
7. Вишневский В.В. Теоретические основы проектирования компьютерных сетей. – М.: Техносфера, 2003. –512 с.
8. Вишневский В., Портной С., Шахнович И. Энциклопедия WiMAX. Путь к 4G. Техносфера. – Москва, 2010. – 470 с.
9. Гельгор А.Л., Попов Е.А. *Гельгор А.Л.* Технология LTE мобильной передачи данных: учеб. пособие. - СПб.: Изд-во Политехн. ун-та, 2011 - 204с.
10. Гепко И.А., Олейник В.Ф., Чайка Ю.Д., Бондаренко А.В. Современные беспроводные сети: состояние и перспективы развития. ЭКМО. - Киев, 2009. – 672 с.
11. Гулевич Д.С. Сети связи следующего поколения. http://www.intuit.ru/department/network/ndnets/)
12. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. – СПб.: БХВ – С-П, 2006. – 368 с.
13. Гольдштейн Б.С., Ехриель И.М., Рерле Р.Д. Интеллектуальные сети. М.: Радио и связь, 2000.
14. Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. Сети связи: Учебник для вузов. - СПб.: БХВ – Петербург, 2010. – 400 с.
15. Б.С. Гольдштейн, А.В. Пинчук, А.Л. Суховицкий. IP-телефония. - М.: Радио и связь- 2001. – 252 с.
16. Гольдштейн А.Б., Гольдштейн Б.С. Технология и протоколы MPLS. - СПб.: БХВ – С-П, 2005. – 304 с.
17. 7. Гук М. Энциклопедия: наиболее полное и подробное руководство «Аппаратные средства локальных сетей». – СПб.: Питер, 2001г. – 576с.
18. Кучерявый А.Е. Гильченок Л.З., Иванов А.Ю. Пакетная сеть связи общего пользования. - СПБ.: Наука и Техника, 2004. – 272 с.
19. Назаров А.Н., Разживин И.А., Симонов М.В. АТМ: Технические решения создания сетей / Под ред. А.Н. Назарова. – М.: Горячая линия – Телеком, 2001. – 376с.
20. Норенков И.П., Трудоношин В.А. Телекоммуникационные технологии и сети. 2– изд., испр. и доп. – М.: МГТУ им. Баумана, 2000. 248с.
21. Олифер В.Г., Олифер Н.А. Новые технологии и оборудование IP-сетей. – СПб.: БХВ – Санкт-Петербург, 2000. – 512с.
22. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010.- 944 с.
23. Попов Е. А. Технология GPRS пакетной передачи данных в сетях GSM : учеб. пособие / Е. А. Попов. - СПб. : Изд-во Политехн. ун-та, 2008. - 182 с.
24. Протоколы информационно-вычислительных сетей. Справочник. Под ред. И. А. Мизина и А. П. Кулешова, Радио и связь, Москва, 1990.
25. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP-телефония. - М.: Эко-Трендз-2003. – 252 с.

26. Семенов Ю.В. Проектирование сетей связи следующего поколения. - СПб.: Наука и Техника, 2005. – 240 с.

27. Семенов Ю. В. Протоколы и ресурсы Internet. - М.: Радио и связь, 1996. - 320 с.: ил.

28. Семенов Ю. В. Сети Интернет: Архитектура и протоколы. - М.: Блик плюс, 1998. - 424 с.

29. Сергиенко А. Б. Цифровая обработка сигналов - СПб.: БХВ - Петербург, 2011. - 768 с.

30. Сети следующего поколения NGN / Под ред. А.В. Рослякова - М.: Эко-Трендз, 2009. – 424 с.

31. Слейдер Й. Эффективное программирование TCP/IP. – СПб.: Питер, 2001. – 320с.

32. 3. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі. –К.: Техніка, 2001.– 392 с.

33. Телекоммуникационные системы и сети. Том 1.- Современные технологии / Под ред. проф. Шувалова В.П. – М.: Горячая линия-Телеком, 2003. – 647 с.

34. Телекоммуникационные системы и сети. Том 3. – Мультисервисные сети / Под ред. проф. Шувалова В.П. – М.: Горячая линия-Телеком, 2005. – 592с.

35. Уолрэнд Дж. Телекоммуникационные и компьютерные сети: Вводный курс/ Пер. с англ. – М.: Постмаркет, 2001. – 480 с.

36. Daniel A. Menascé, Virgilio A.F. Almeida. Capacity Planning for Web Services: Metrics, Models, and Methods. 2001. - Published Sep 11, 2001 by Prentice Hall.- 608.

37. Held, Gilbert. Ethernet networks: design, Implementation, operation, management/. – 2nd ed. Wiley professional computing, New York, 1996.

38. Srinivas Vegesna. IP Quality of Service. 2003. - Cisco Press. – 368c.

39. W. Richard Stevens. TCP/IP Illustrated, Volume 1. 1993/ Addison-Wesley. – 538 с.

40. Vivek Alwayn. Advanced MPLS Design and Implementation. 2004. -Cisco Press. – 408.

41. ITU-T Recommendation H.248. Gateway control protocol. - Geneva, 2000.

42. ITU-T Recommendation H.320. Narrow-band Visual Telephone Systems and Terminal Equipment. - 1996.

43. ITU-T Recommendation H.321. Adaptation of H.320 Visual Telephone Terminals to B-ISDN Environments. - 1996.

44. ITU-T Recommendation H.322. Visual Telephone Systems and Terminal Equipment for Local Area Networks which Provide a Guaranteed Quality of Service. - 1996.

45. ITU-T Recommendation H.323. Packet based multimedia communication systems. - Geneva, 1998.

46. RFC 2705. Media Gateway Control Protocol (MGCP) Version 1.0. M. Arango, A. Dugan, I. Elliott, C. Huitema, S. Pickett. October 1999.

47. RFC 2865. Remote Authentication Dial In User Service (RADIUS). C.Rigney, S. Willens, A. Rubens, W. Simpson. June 2000.

48. RFC 2885. Megaco Protocol 0.8. F Cuervo, N. Greene, C. Huitema, A.Rayhan, B. Rosen, J. Segers. August 2000.

49. Toga J., Ott J. ITU-T standardization activities for interactive multimedia communications on packet-based networks: H.323 and related recommendations / Computer Networks, 1999.