ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ ТА МЕРЕЖ

КВАЛІФІКАЦІЙНА РОБОТА

на тему: «ПОБУДОВА МЕРЕЖ IP-ТЕЛЕФОНІЇ НА БАЗІ ПРОТОКОЛУ SIGTRAN»

на здобуття освітнього ступеня магістр
зі спеціальності 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело.

_____ Віталій СТЕЦЮК
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Виконав: здобувач вищої освіти гр. ТСДМ-63
Віталій СТЕЦЮК
Ім'я, ПРІЗВИЩЕ

Керівник: Костянтин ЛАВРІНЕЦЬ
к.т.н., доцент *Ім'я, ПРІЗВИЩЕ*

Рецензент: _____
Ім'я, ПРІЗВИЩЕ

Київ 2025

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут Телекомунікацій

Кафедра ___Телекомунікаційних систем та мереж_____
Ступінь вищої освіти __магістр_____
Спеціальність ___172 Електронні комунікації та радіотехніка
Освітньо-професійна програма _____Телекомунікаційні системи та мережі

ЗАТВЕРДЖУЮ
Завідувач кафедрою __ТСМ_____
_____ Віктор ЗАЇКА
«____» _____ 2025 р.

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Стецюку Віталію Романовичу
(прізвище, ім'я, по батькові здобувача)

1. Тема кваліфікаційної роботи: Побудова мереж IP- телефонії на базі протоколу SIGTRAN
керівник кваліфікаційної роботи Костянтин ЛАВРІНЕЦЬ, к.т.н., доцент
(Ім'я, ПРІЗВИЩЕ науковий ступінь, вчене звання)
затверджені наказом Державного університету інформаційно-комунікаційних технологій від « ___ » ____2025 р. № ___.

2. Строк подання кваліфікаційної роботи «___» _____ 2025 р.

3. Вихідні дані до кваліфікаційної роботи:
1.Сигналізація у мережах IP-телефонії
2.Протоколи з декомпозицією шлюзів
3.Архітектура SIGTRAN
4. Характеристика протоколів адаптаційних рівнів SIGTRAN.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити)
1.Керування дзвінками в мережі IP-телефонії
2.Архітектура мережі, що базується на протоколі MGCP
3. Архітектура протоколу Sigtran
4. Архітектура мережі з використанням протоколу Sigtran

5. Перелік ілюстративного матеріалу: ___презентація на слайдах_____

6. Дата видачі завдання «___» _____ 2025 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1	Підбір та аналіз науково-технічної літератури	10.10.2025	Викон.
2	Сигналізація у мережах IP-телефонії	20.10.2025	Викон.
3	Протоколи з декомпозицією шлюзів	31.10.2025	Викон.
4	Архітектура протоколу Sigtran	20.11.2025	Викон.
5	Висновки, вступ, реферат	30.11.2025	Викон.
6	Розробка презентації	15.12.2025	Викон.

Здобувач вищої освіти _____ Віталій СТЕЦЮК
(підпис) *(Ім'я ПРІЗВИЩЕ)*

Керівник кваліфікаційної роботи _____ Костянтин ЛАВРІНЕЦЬ
(підпис) *(Ім'я ПРІЗВИЩЕ)*

ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
Навчально-науковий інститут телекомунікацій
ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ
на здобуття освітнього ступеня магістра

Направляється здобувач Стецюк В. Р. до захисту кваліфікаційної роботи
(прізвище та ініціали)
за спеціальністю 172 Електронні комунікації та радіотехніка
(код, найменування спеціальності)
освітньо-професійної програми Телекомунікаційні системи та мережі
(назва)
на тему: «: Побудова мереж IP- телефонії на базі протоколу SIGTRAN ».

Кваліфікаційна робота і рецензія додаються.

Директор ННІТ _____ Владислав КРАВЧЕНКО
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

Висновок керівника магістерської роботи

Здобувач Стецюк Віталій Романович показав гарну теоретичну та інженерну підготовку, уміння володіти новими комп'ютерними технологіями, користуватися навчальною, довідковою і науково-технічною літературою. Працюючи над завданнями, які були поставлені керівником, проявив ініціативність, сумлінність та хист до наукової роботи.

Все це дозволяє оцінити виконану кваліфікаційну роботу здобувача Стецюка Віталія Романовича на оцінку «добре» та присвоїти йому кваліфікацію магістр з електронних комунікацій та радіотехніки.

Керівник кваліфікаційної роботи _____ Костянтин ЛАВРІНЕЦЬ
(підпис) *(Ім'я, ПРІЗВИЩЕ)*

«____» _____ 2025 року

Висновок кафедри про магістерську роботу

Кваліфікаційна робота розглянута. Здобувач Стецюк В. Р. допускається до захисту даної роботи в Екзаменаційній комісії.

Завідувач кафедрою телекомунікаційних систем та мереж _____ Віктор ЗАЇКА
(назва) *(підпис)* *(Ім'я, ПРІЗВИЩЕ)*

ВІДГУК РЕЦЕНЗЕНТА
на кваліфікаційну роботу
на здобуття освітнього ступеня магістра

здобувача вищої освіти Стецюка Віталія Романовича
(прізвище, ім'я, по батькові)
на тему «Побудова мереж IP- телефонії на базі протоколу SIGTRAN »

Актуальність.

Проведений аналіз протоколу SIGTRAN показав можливість його використання при побудові комутаторів Softswitch , який склав хорошу альтернативу системам управління обслуговуванням викликів у традиційних АТС як за ціною та функціональними можливостями, так і за масштабованістю, якістю обслуговування, габаритами, енергоспоживанням та вартістю технічної експлуатації. Тому тема актуальна.

Позитивні сторони.
В магістерській кваліфікаційній роботі показано, що на основі побудови мереж IP-телефонії можливо істотно скоротити смугу пропускання для передачі мови, відео та даних в режимі мультимедійних повідомлень і істотно зменшити завдяки цьому вартість надаваних послуг абонентам.

Недоліки.

1. Треба було більш детально провести порівняльний аналіз з іншими протоколами.
2.Слід було більше уваги приділити технічним засобам, їх технічним характеристикам, та виконати порівняльний аналіз.

Відзначені зауваження не впливають на загальну позитивну оцінку бакалаврськоїкваліфікаційної роботи

Висновок: *кваліфікаційна робота на здобуття ступеня магістра заслуговує оцінку "добре", а здобувач* Стецюк Віталій Романович *заслуговує присвоєння кваліфікації: магістр з електронних комунікацій та радіотехніки.*

Рецензент
науковий ступінь, вчене звання _____ (підпис) _____ *(Ім'я ПРІЗВИЩЕ)*

РЕФЕРАТ

Текстова частина кваліфікаційної роботи на здобуття освітнього ступеня магістра: ___ стор., ___ рис., ___ табл., ___ джерел.

Об’єкт дослідження – сигналізація у мережі IP-телефонії.

Предмет дослідження – дослідження принципів побудови мереж IP-телефонії з використанням протоколу SIGTRAN.

Мета роботи – розробити методику побудови мереж IP-телефонії з використанням протоколу SIGTRAN.

Проведений аналіз протоколу SIGTRAN показав можливість його використання при побудові комутаторів Softswitch , який склав хорошу альтернативу системам управління обслуговуванням викликів у традиційних АТС як за ціною та функціональними можливостями, так і за масштабованістю, якістю обслуговування, габаритами, енергоспоживанням та вартістю технічної експлуатації. Але основна причина успіху Softswitch - його вміння узгоджувати різні протоколи сигналізації як мереж одного типу, наприклад, при поєднанні мереж H .323 і SIP , так і при взаємодії мереж комутації каналів (протоколи ОКС 7) з IP -мережами (протоколи SI P MGCP Megaco / H.248 , BICC), яке розглядається із застосуванням технології SIGTRAN, що підтримує підсистеми ОКС 7 засобами IP -протоколів. Ранні програми передачі мови поверх IP (IP - телефонії) викликали сумнів з погляду якості обслуговування (QoS). Численні вдосконалення ¬IP - мереж, пов'язані, зокрема, з розвитком технології MPLS , зараз забезпечують якість обслуговування не гірше, ніж системи комутації каналів у ТФОП. Взаємозв'язок мереж Про КС 7 та IP , яка потрібна при проходженні викликів як через мережу ТФОП, так і через мережу IP є важливою проблемою. У цьому питанні досягнуто великого успіху, зокрема завдяки новій технології, призначеній для роботи з мережами IP і відомої як технологія SIGTRAN. Ця технологія емулює Про КС 7 засобами IP -протоколів. Принципи побудови мереж IP-телефонії дозволяють істотно скоротити полосу пропускання для передачі мови, відео та даних в режимі мультимедійних повідомлень і істотно зменшити завдяки цьому вартість надаваних послуг абонентам. Сімейство протоколів SIGTRAN забезпечує можливість передачі мовних повідомлень, відео та даних по мережах IP-телефонії та добре інтегрується з можливостями ТМЗК.

КЛЮЧОВІ СЛОВА:

КОМУТАЦІЯ КАНАЛІВ, КОМУТАЦІЯ ПАКЕТІВ, СТЕК ПРОТОКОЛІВ TCP/IP, IP-ТЕЛЕФОНІЯ, ПРОТОКОЛ H-323 , ПРОТОКОЛ H - 248, MGCP , МОЖЛИВОСТІ ВИКОРИСТАННЯ МЕРЕЖ IP-ТЕЛЕФОНІЇ.

ABSTRACT

Text part of the qualification work for the degree of Master: ___ pages, ___ figures, ___ tables, ___ sources.

The object of the study is signaling in the IP-telephony network.
The subject of the study is the study of the principles of building IP-telephony networks using the SIGTRAN protocol.
The purpose of the work is to develop a methodology for building IP telephony networks using the SIGTRAN protocol.
The analysis of the SIGTRAN protocol showed the possibility of its use in building Softswitch switches, which was a good alternative to call management systems in traditional PBXs.
both in terms of price and functionality, as well as scalability, quality of service, size, power consumption and cost of technical operation. But the main reason for the success of Softswitch is its ability to coordinate different signaling protocols as networks of the same type, for example, when combining networks H.323 and SIP, and in the interaction of circuit switching networks (OKC 7 protocols) with IP networks (SI P MGCP Megaco / H.248, BICC protocols), which is considered using SIGTRAN technology, which supports OKC 7 subsystems by means of IP protocols. Early voice over IP (IP- telephony) have raised doubts in terms of quality of service (QoS). Numerous improvements in ¬IP networks, associated, in particular, with the development of MPLS technology, now provide quality of service no worse than circuit switching systems in PSTN. Network Interconnection About KC 7 and IP, which is required when passing
calls over both PSTN and IP networks is a significant problem. Much progress has been made in this area, in particular through a new technology designed for IP networks known as SIGTRAN. This technology emulates Pro KC 7 using IP protocols. Principles of Networking IP telephony allows to significantly reduce the bandwidth for the transmission of voice, video and data in the mode of multimedia messages and thereby significantly reduce the cost of services provided to subscribers. The SIGTRAN family of protocols provides the ability to transmit voice messages, video and data over IP telephony networks and integrates well with the capabilities of TMZK.

KEYWORDS:

CHANNEL SWITCHING, PACKET SWITCHING, TCP/IP PROTOCOL STACK, IP TELEPHONY, H-323 PROTOCOL, H - 248 PROTOCOL, MGCP, POSSIBILITIES OF USING IP TELEPHONY NETWORKS.

ЗМІСТ

ВСТУП ……9

1.СИГНАЛІЗАЦІЯ У МЕРЕЖАХ IP-ТЕЛЕФОНІЇ……..……13
1.1.Загальні принципи сигналізації в мережах IP-телефонії ……13
1.2.Сигналізація за стандартомH-323……..16
1.3.Сигналізація на основі протоколу SIP… ……..26
1.4.Порівняння протоколів H-323 і SIP……...30
1.5.Особливостісигналізації за концепцією TIPHON ……...32
2.ПРОТОКОЛИ З ДЕКОМПОЗИЦІЄЮ ШЛЮЗІВ……35
2.1.Загальна характеристика протоколів MGCP і Megaco …….35
2.2.Протокол MGCP …….36
2.2.1.Архітектура мережі за протоколом MGCP ……...36
2.2.2.Встановлення, зміна та руйнування сполук……...37
2.3.Протокол Megaco ……40
2.3.1. Архітектура мережі за протоколом Megaco …….40
2.3.2.Приклад встановлення та руйнування з'єднання за протоколом Megaco ……....41
2.4.Межсетевое взаємодія……47
2.5.Порівняльний аналіз протоколів MGCP і Megaco ……..49
3.АРХІТЕКТУРА SIGTRAN ……..…..54
3.1.Рівні моделі Sigtran у стеку протоколів TCP/IP……..…...54
3.2.Адаптивні рівні Sigtran……..……..55
3.3.Транспортний протокол з керованим потоками…….....57
3.3.1.Основні функціональні можливості……...….57
3.3.2.Множинна адресація……...…..58
3.3.3.Сполуки кількох потоків……60
3.3.4.Фрагменти……..62
3.3.5.Фрагмент корисного навантаження DATA ……...…69
3.3.6.Встановлення сполуки……..70
4. ХАРАКТЕРИСТИКА ПРОТОКОЛОВ АДАПТАЦІЙНИХ РІВНІВ S IGTRAN ……..…74
4.1.Функції протоколу M3UA… ……74
4.2.Термінологія протоколу ……...…..75
4.3.Код пункту сигналізації……..…76
4.4.Примітиви…….....77
4.5. Повідомлення протоколу M3UA……...…78
4.6.Протокол M2UA……...…82
4.7.Протокол M2PA……84
4.8.Протокол SUA… ……87
4.9.Протокол IUA…….91
4.10.Протокол V 5 UA ……92
4.11.Приклади мережевих конфигураций……..…..92
ВИСНОВКИ……..... 96
ПЕРЕЛІК ПОСИЛАНЬ……...97
ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ……98

ВСТУП

Досягнення електронної техніки за останнє десятиліття призвели до справжнього буму в галузі телекомунікацій. Зв'язок, що знаходиться в статичному стані ще з середини 1980-х років, сьогодні перетворилася на галузь, що бурхливо розвивається, що приносить операторам значні прибутки.

Користувачі отримали доступ до послуг, про які 10–15 років тому не замислювалися. E-mail, Інтернет, мобільний телефон стали звичайними атрибутами повсякденного життя. Користувачеві вже досить просто поговорити по домашньому телефону. Ми хочемо мати можливість зателефонувати своїм друзям, перебуваючи на вулиці, в поїзді, на кораблі, в будь-якій точці земної кулі.

Нам уже недостатньо мати кілька різних номерів, що належать до різних мереж (телефонна мережа загального користування, мобільна мережа, Інтернет і т.д.). Ми хочемо мати один персональний номер, який дозволяв би однозначно визначати нас і спрямовувати вхідний дзвінок до терміналу, підключеного до мережі, де ми перебуваємо в даний момент.

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

- якнайшвидше і дешевше створювати нові послуги, щоб постійно залучати нових абонентів;
- зменшувати витрати на обслуговування;
- бути незалежними від постачальників обладнання;
- бути конкурентоспроможними

Технологічною основою інформаційного суспільства є **Глобальна інформаційна інфраструктура (ДІІ)** , яка має забезпечити можливість доступу

до інформаційних ресурсів кожного мешканця планети. Інформаційну інфраструктуру складає сукупність баз даних, засобів обробки інформації, взаємодіючих мереж зв'язку та терміналів користувача.

Доступ до інформаційних ресурсів у ДІІ реалізується за допомогою послуг зв'язку нового типу, які отримали назву послуг Інформаційного товариства або **інфокомунікаційних послуг** .

Високі темпи зростання обсягів надання інфокомунікаційних послуг, що спостерігаються в даний час, дозволяють прогнозувати їх переважання в мережах зв'язку в найближчому майбутньому.

Сьогодні розвиток інфокомунікаційних послуг здійснюється, переважно, у межах комп'ютерної мережі Інтернет, доступом до послуг якої відбувається через традиційні мережі зв'язку.

Водночас у ряді випадків послуги Інтернету через обмежені можливості її транспортної інфраструктури не відповідають сучасним вимогам, що пред'являються до послуг інформаційного суспільства.

До інфокомунікаційних послуг висуваються такі вимоги, як:

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

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

Найважливішим стимулом ринкового успіху інфокомунікаційних послуг з'явилися досягнення в галузі розвитку засобів сигналізації, можливість

перетворювати *сигналізацію за протоколами* як мереж одного типу, наприклад, при поєднанні мереж H .323 і SIP , так і різнотипних мереж, наприклад, при поєднанні мереж з комутацією каналів (протоколи стека ОКС 7) та IP -мереж (протоколи SIP , MGCP , MEGACO / H.248 , H.323). Ця здатність з'явилася завдяки введенню нового мережевого елемента Softswitch , яка зберігається при організації спільної роботи транспортних шлюзів різних постачальників.

Незважаючи на суттєвий прогрес у стандартизації SIP і *H .323,* взаємодія різнорідного мережевого обладнання все ще залишається важкою. Те саме справедливо і щодо протоколів управління транспортними шлюзами *MGCP , MEGACO / H.248* .

Застосування Softswitch дозволяє подолати проблеми взаємодії між собою транспортних шлюзів з різними системами сигналізації. Основною такою системою за сьогоднішньої конвергенції мереж та послуг зв'язку є система загальноканальної сигналізації *№7(ОКС7), що* розглядається із застосуванням Softswi tch . Взаємозв'язок мереж ОКС 7 і IP , яка потрібна при проходженні дзвінків як через мережу ТФОП, так і через мережу IP , є важливою проблемою. У цьому питанні досягнуто великого успіху, зокрема завдяки новій технології, призначеній для роботи з мережами IP і відомої як технологія **Sigtran .**

У дипломній роботі розглянемо архітектуру, можливості та функціональні - вимоги до протоколу SIGTRAN для транспортування сигнальних повідомлень. У частині архітектури розглядаються взаємозв'язки між функціональними та фізичними об'єктами, що використовуються для транспортування сигнальної інформації, включаючи конфігурацію керування транспортними шлюзами . Gateway) та інші сценарії, де може вимагатися транспортування сигнальної інформації.

У частині вимог описуються функціональні та якісні вимоги до транспортування сигнальної інформації, наприклад, управління потоком,

послідовності доставки та інших функцій, які можуть бути потрібні для конкретних протоколів сигналізації мережі з комутацією каналів.

У роботі також розглядаються основні положення щодо застосування протоколу передачі інформації управління потоком (Stream Control Transmission Protocol — SCTP), розробленого робочою групою IETF SIGTRAN , для транспортування сигнальної інформації через інфраструктуру мережі IP . Наведено відомості щодо специфіки транспортування інформації сигналізації через мережу IP (адресація, маршрутизація). Розглядається використання адаптаційних рівнів, необхідних для транспортування сигналізації із застосуванням протоколу SCTP .

1 СИГНАЛІЗАЦІЯ У МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

1.1 Загальні принципи сигналізації у мережах IP-телефонії

Для забезпечення широкомасштабного впровадження IP-телефонії одним із найважливіших факторів є забезпечення сумісності систем різних фірм. Досягнення сумісності можливе лише з урахуванням стандартних протоколів сигналізації. Протоколи сигналізації забезпечують встановлення, адміністрування та завершення сеансу зв'язку між кінцевими точками, що однозначно ідентифікуються заданою схемою адресації. Поняття «сигналізація» стосується всієї інформації, пов'язаної з викликами та необхідної для їх встановлення, маршрутизації, моніторингу та завершення як на фізичному, так і на логічному рівні.

У традиційній телефонії абонент набирає номер потрібного йому абонента, а телефонна мережа використовує його для маршрутизації виклику. Процедура керування викликами поділяється на три фази: встановлення з'єднання, передача мови або даних та роз'єднання. Повідомлення системи сигналізації ініціюють та завершують ці фази, а стандартні контрольні сигнали та (або) записані голосові повідомлення інформують абонента про характер проходження його виклику.

У всіх сучасних мережах з комутацією каналів система сигналізації заснована на сімействі ГКС №7. Вони забезпечують обмін повідомленнями, які необхідні маршрутизації викликів, резервування ресурсів, трансляції адрес, встановлення з'єднань, управління ними, виставлення рахунків. У порівнянні з сигналізацією у звичайних телефонних мережах сигналізація IP-телефонії повинна мати більш широкі можливості в силу специфіки кінцевих вузлів. Вони можуть мати різні характеристики в частині необхідної смуги пропускання, кодування/декодування аудіосигналів, передачі даних і т.д., і для встановлення сеансу зв'язку між ними необхідно переконатися в сумісності цих характеристик.

У системах IP-телефонії процедури керування викликами виконуються протоколами сигналізації, а безпосередня маршрутизація трафіку через IP-мережу

забезпечується протоколами: OSPF або BGP (резервування мережевих ресурсів можливе, наприклад, за допомогою протоколу RSVP). Таким чином, архітектура мережі IP-телефонії передбачає поділ площин управління та передачі інформації користувача, що є найбільш сприятливою умовою для впровадження нових послуг (рис. 1.1).

В даний час ще остаточно не вирішено питання вибору оптимальної архітектури керування викликами особливо для Інтернет-телефонії: чи має бути інтегрована з існуючими службами Інтернет або розгорнута окремо для забезпечення управління в режимі реального часу. Перший підхід залучає Інтернет-провайдерів, які розглядають послуги Інтернет-телефонії лише як невелику частину свого пакета сервісу. Вони планують пропонувати ці послуги за фіксованими тарифами, використовуючи максимально спрощену схему управління послугами. За другий підхід ратують оператори, для яких Інтернет-телефонія є основною або навіть єдиною послугою, що пропонується. Їм необхідні системи, здатні забезпечити високий рівень контролю за використанням мережевих ресурсів та потужні засоби білінгу.

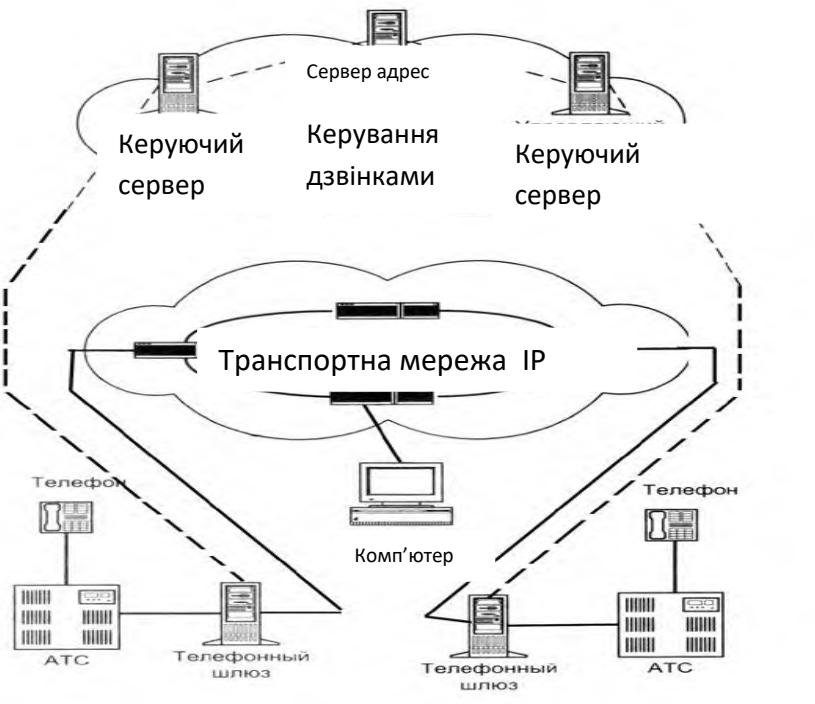


Рис.1.1 Керування дзвінками в мережі IP-телефонії

Ще одне важливе питання, пов'язане із сигналізацією в IP-телефонії - контроль за доступом до мережі. У звичайній телефонній мережі загального користування (ТФЗП) абонент підключається до АТС через фіксований місцевий шлейф, тому ідентифікувати його телефонний апарат дуже просто. У мережі IP-телефонії все набагато складніше, оскільки існує безліч різних способів доступу до неї: зі звичайного телефону через ТФОП, модемного з'єднання через сервер віддаленого доступу, через ЛОМ і територіально розподілену мережу і т.д. Крім цього, користувачі можуть переміщатися між різними мережами, таким чином, абонента не можна ідентифікувати по лінії доступу, що використовується. Для ефективного контролю за доступом оператор повинен автентифікувати кожного користувача, який запитує послугу. Зі збільшенням числа операторів IP-телефонії потрібні також засоби контролю за трафіком на кордоні між мережами. Такі засоби повинні здійснювати контроль за доступом та використанням мережевих ресурсів та виконанням угод щодо якості обслуговування. За їх відсутності оператору може бути проблематичним гарантувати користувачеві певний клас обслуговування, якщо його трафік частково проходить через мережу іншого оператора.

На рис. 1.2 показано місце механізмів сигналізації IP-телефонії у протокольному стеку: з них перебувають програми, під ними - транспортні служби IP. Програма може являти собою телефонний шлюз.

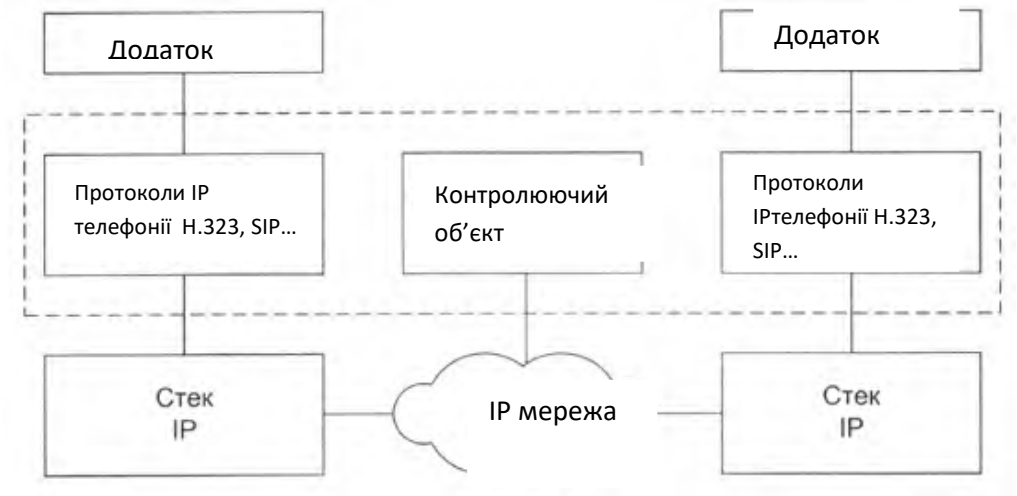


Рис. 1.2 Механізми сигналізації IP-телефонії у протокольному стеку

У загальному випадку для встановлення з'єднання між абонентом, що викликається, і шлюзи IP-телефонії повинні:

- знайти gatekeeper, на якому можлива реєстрація кінцевого пристрою;
- зареєструвати свою мнемонічну адресу на gatekeeper;
- вказати необхідну смугу пропускання;
- передати запит на встановлення з'єднання;
- встановити з'єднання;
- у процесі виклику керувати параметрами з'єднання;
- роз'єднати з'єднання.

На виконання цих операцій у час можуть використовуватися різні протоколи сигналізації, розглянуті нижче.

1.2 Сигналізація за стандартом H.323

Рекомендація Міжнародного союзу електрозв'язку (МСЕ-Т) H.323 визначає основи процесу передачі аудіо, відео та даних по мережах з комутацією пакетів, наприклад мереж IP. В ній описані об'єкти, необхідні для мультимедійного зв'язку, їх функції та способи взаємодії, зокрема алгоритми формування пакетів, стиснення аудіо- та відеоінформації. Крім того, рекомендація H.323 націлена на вирішення завдань адміністрування кінцевих користувачів, адресації, контролю за використанням смуги пропускання мережі та мережевих об'єктів.

В даний час дійсна версія 5 H.323 - це рекомендація, в якій описані компоненти мережі та надано рекомендації до застосування безлічі додаткових рекомендацій. Усі разом ці рекомендації часто називають сімейством H.323 (рис. 1.3).

Деякі компанії домагаються включення в H.323 підтримки мультимедіа-можливостей, заснованих на запропонованому протоколі IETF Session Initiation Protocol. Версія доповнена засобами, що дозволяють враховувати параметри сеансів для цілей тарифікації, а також підтримкою каталогів - замість цифрових IP-адрес можна користуватися іменами.

Для виконання дій сигналізації між шлюзами та gatekeeper відповідно до Рекомендації МСЕ-Т H.323 використовуються такі протоколи:

- сигналізація RAS (Registration, Admission, Status);
- сигналізація Q.931 (згідно з H.225.0);
- протокол керування H.245.

Сигналізація RAS

Протокол сигналізації RAS (реєстрації, підтвердження та стану) застосовується для передачі службових повідомлень між терміналами та контролером зони

H.323. RAS-повідомлення служать для реєстрації терміналів, допуску їх до сеансу зв'язку, зміни смуги пропускання, що використовується, інформування про стан сеансу і його припинення. У відсутності контролера зони (gatekeeper) протокол RAS не використовується.

Функції сигналізації RAS використовують повідомлення протоколу H.225.0. Канал сигналізації RAS залежить від каналу управління викликом і каналу управління H.245.

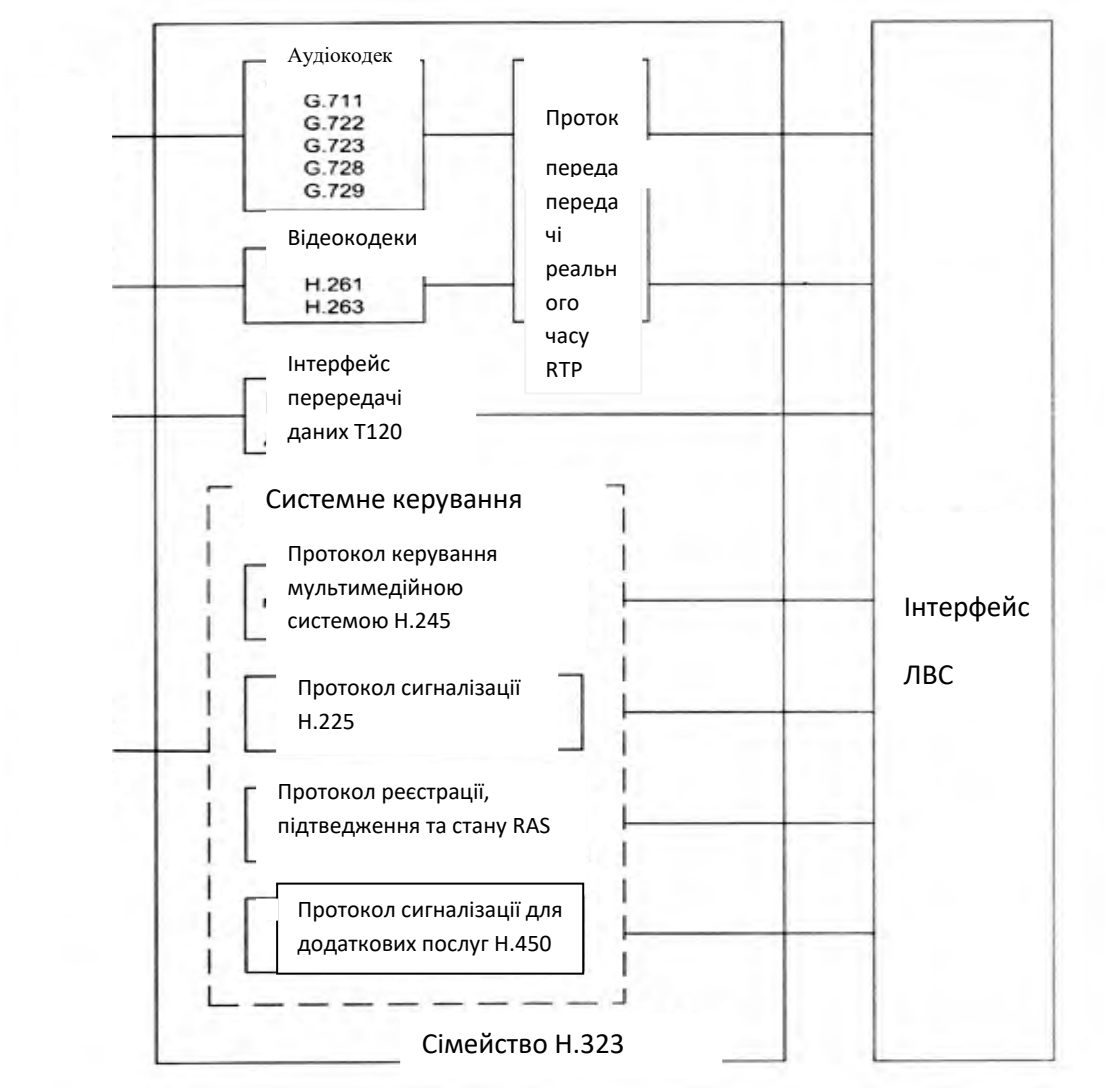


Рис. 1.3 Сукупність рекомендацій H.323

За допомогою сигналізації RAS має здійснюватися:

- знаходження gatekeeper, на якому можлива реєстрація кінцевого обладнання;
- реєстрація кінцевого пристрою;

- визначення географічного положення кінцевого пристрою;
- вказівку необхідної смуги пропускання;
- зміна смуги пропускання.

Надсилання повідомлень RAS здійснюється в дейтаграмах UDP. Для адресації RAS має використовуватися адресна інформація, до якої входять:

- мережеву адресу обладнання;
- ідентифікатор TSAP (Transport Layer Service Access Point);
- мнемонічна адреса (Alias Address).

Мережева адреса є адресою у форматі, що використовується в мережі з комутацією пакетів, наприклад, адреса у форматах IPv4, IPv6, IPX, NetBIOS.

Ідентифікатор TSAP використовується для ідентифікації інформаційних потоків, надісланих з однієї адреси мережі. Для gatekeeper виділено постійні значення ідентифікатора TSAP: 1718 (для пошуку gatekeeper) та 1719 (для передачі повідомлень сигналізації RAS).

Мнемонічна адреса служить для адресації кінцевого обладнання зручній користувачеві формі. Адреса може бути телефонний номер у форматі E.164, телефонний номер у корпоративній мережі, адреса електронної пошти і т.д. Gatekeeper не має менімонічної адреси.

Знаходження gatekeeper повинно здійснюватися за допомогою широкомовного запиту GRQ (Gatekeeper Request), що передається кінцевим обладнанням з ідентифікатором TSAP, рівним 1718. Якщо gatekeeper знайдено, і він готовий обслужити запит від кінцевого обладнання, у відповідь воно має отримати повідомлення GCF (G). Якщо кінцеве обладнання отримало відповідь від кількох gatekeeper, вибір одного з них повинен здійснюватися кінцевим обладнанням довільним чином. Якщо gatekeeper не може обслужити запит від кінцевого обладнання, то у відповідь він повинен передати повідомлення GRJ (Gatekeeper Reject), в якому повинна повідомлятися причина відмови, і може бути адреса альтернативного gatekeeper. При знаходженні gatekeeper між ним і кінцевим обладнанням здійснюється встановлення логічного каналу сигналізації, яким будуть передаватися інші повідомлення RAS (рис. 1.4).

Після знаходження gatekeeper кінцеве обладнання в повідомленні RRQ (Registration Request) має повідомити gatekeeper свою мережеву та мнемонічну адресу. У відповідь gatekeeper повинен передати повідомлення RCF (Registration Confirm) на підтвердження реєстрації кінцевого обладнання, або RRJ (Registration Reject) у разі відмови від реєстрації. Повідомлення RRQ може надсилатися при включенні кінцевого обладнання. Якщо при повторній реєстрації менімонічна та мережева адреси, передані gatekeeper кінцевим обладнанням, збігаються з раніше переданими, то gatekeeper повинен передати повідомлення RCF. Якщо при повторній реєстрації менімонічна адреса дорівнює раніше вказаній, а мережеві відрізняються, має бути передано повідомлення RRJ з причиною відмови duplicate registration. Для скасування реєстрації використовуються повідомлення URQ (Unregistered Request), що передається кінцевим обладнанням, і UCF (Unregistered confirm), URJ (Unregistered reject), що передаються gatekeeper кінцевого обладнання.

Реєстрація кінцевого обладнання на gatekeeper може здійснюватися один раз і не повторюватися при включенні кінцевого обладнання. У цьому випадку gatekeeper повинен визначати стан кінцевого обладнання. Для цього gatekeeper має періодично передавати повідомлення IRQ (Information Request).



Рис. 1.4 Етапи проходження виклику серед H.323

Інтервал визначається виробником обладнання та має бути не менше 10 секунд.

Після реєстрації кінцевого обладнання на gatekeeper воно може встановити з'єднання з викликаним кінцевим обладнанням. Для цього кінцеве обладнання-ініціатор має передати повідомлення ARQ (Admissions Request) та встановити логічний канал для передачі повідомлень Q.931. У повідомленні ARQ вказуються швидкість передачі, кратна 100 біт/с, та кількість каналів, необхідних передачі мовної інформації. Наприклад, при використанні інтерфейсів ISDN для виділення смуги 192 кбіт/с необхідно вказати значення відповідно 640 та 3. Швидкість вказується без урахування розмірів заголовків пакетів та блоків даних

транспортних протоколів. Якщо мережа може забезпечити необхідні параметри, то gatekeeper повинен передати підтвердження ACF (Admissions Confirm), інакше передається повідомлення ARJ (Admissions Reject) із зазначенням причини відмови.

Після отримання підтвердження кінцеве обладнання встановлює з'єднання з кінцевим обладнанням, що викликається з використанням сигналізації Q.931 (відповідно до H.225.0). Повідомлення сигналізації Q.931 можуть передаватися логічним каналом через gatekeeper або безпосередньо між двома кінцевими пристроями. Вибір способу здійснює gatekeeper і повідомляє про це кінцеве обладнання в повідомленні ACF.

Якщо повідомлення передаються через gatekeeper, то він може або закрити логічний канал після встановлення з'єднання передачі мовної інформації, або залишити його до кінця сеансу зв'язку, якщо підтримуються додаткові послуги.

Для встановлення з'єднання використовуються повідомлення Setup та Connect, після передачі яких встановлюється канал керування H.245. Канал передачі інформації управління H.245 може бути встановлений двома способами: через gatekeeper або безпосередньо між кінцевими пристроями. У разі, якщо логічний канал сигналізації Q.931 встановлюється через gatekeeper, то канал передачі інформації управління H.245 також повинен встановлюватися через gatekeeper. Спосіб встановлення каналу передачі інформації управління H.245 між кінцевим обладнанням в даний час не специфікований.

Якщо канал сигналізації RAS встановлено, він може використовуватися для встановлення декількох з'єднань. Ідентифікація повідомлень сигналізації, що належать одному й тому з'єднанню, здійснюється за допомогою ідентифікатора Call ID.

Сигналізація H.225.0 (Q.931) та протокол управління H.245

Стандарт H.225 описує протоколи сигналізації та формування пакетів у системах пакетної передачі мультимедійного трафіку. Канал управління викликами H.225.0 використовується для встановлення та розриву з'єднань між двома терміналами H.323, а також між терміналом та шлюзом. Службові повідомлення цього протоколу передаються поверх TCP чи UDP (рис. 1.5). Відповідний механізм H.225.0 заснований на протоколі Q.931, розробленому для мереж ISDN. Він забезпечує надання цілого ряду додаткових видів обслуговування та можливість взаємодії з мережами, що базуються на комутації каналів. Канал управління викликом залежить від каналу RAS і каналу управління H.245.

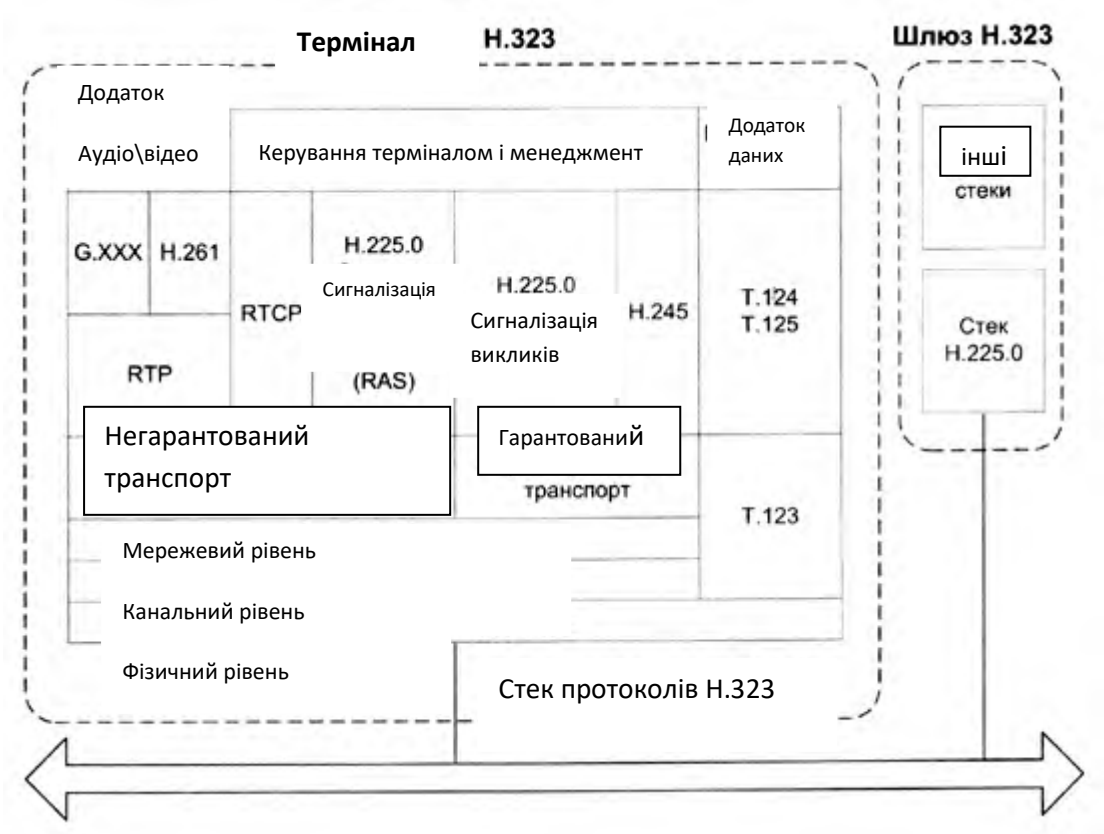


Рис. 1.5 Положення H.225.0 у стеку протоколів H.323

Рекомендація H.245 визначає синтаксис та семантику термінальних сигнальних повідомлень, а також процедур, що використовуються для передачі їх у смузі розмови на початку або протягом сеансу зв'язку. Визначено процедури

підтвердження сигнальної інформації для забезпечення гарантії надійної передачі аудіовізуальної інформації та даних.

Рекомендація охоплює широкий спектр програм, включаючи зберігання/повторну передачу, передачу повідомлень та розподіл послуг, а також забезпечення діалогу. Це стосується систем передачі всіх видів інформації, які використовують методи мультиплексування, визначені в Рекомендаціях H.222.0, H.223 і H.225.0.

Протокол управління мультимедійною передачею H.245 забезпечує:

- узгодження можливостей компонентів;
- встановлення та розрив логічних каналів;
- передачу запитів встановлення пріоритету;
- керування потоком (завантаженням каналу);
- передачу загальних команд та індикаторів.

Повідомлення протоколу H.245 передаються спеціальним каналом управління. Це логічний канал «О», який, на відміну від каналів обміну мультимедіа потоками, постійно відкритий. Обмін параметрами між терміналами дозволяє узгоджувати режими роботи та формати кодування інформації, що забезпечує взаємодію терміналів від різних виробників. У процесі обміну повідомленнями про параметри уточнюються можливості терміналів приймати та передавати різні види трафіку.

За допомогою сигналізації Q.931 згідно з рекомендацією МСЕ-Т H.225.0 та протоколом управління H.245 повинно здійснюватися:

- передача запиту встановлення з'єднання;
- ініціалізація з'єднання та обмін інформацією про можливості;
- встановлення з'єднання передачі мовної інформації;
- роз'єднання з'єднання.

Для встановлення з'єднання ініціатор виклику (кінцеве обладнання 1) має передати повідомлення Setup кінцевого обладнання 2 по логічному каналу сигналізації з ідентифікатором TSAP, рівним 1719.

У відповідь одержувач (кінцеве обладнання 2) повинен передати повідомлення Connect, яке повідомляє ініціатору про готовність встановити з'єднання. Ініціатор повідомлення повинен отримати повідомлення Call proceeding, Connect, Alerting протягом 4 секунд.

Після отримання повідомлення Connect повинен бути встановлений логічний канал управління H.245, яким передається інформація про можливості кінцевого обладнання в повідомленні terminal Capability Set.

Для визначення ініціатора встановлення каналу RTP використовується ідентифікатор status Determination Number у повідомленні Master Slave Determination. Після ініціалізації з'єднання створюється логічний канал передачі мовної інформації. Встановлення каналу передачі мовної інформації здійснюється кінцевим обладнанням після отримання повідомлення open Logical Channel каналом управління H.245. Передача мовної інформації логічним каналом повинна здійснюватися в пакетах RTP. Передача керуючої інформації має здійснюватися у пакетах RTCP.

При необхідності змінити необхідну смугу пропускання використовується повідомлення BRQ (Bandwidth Change Request) сигналізації RAS, яке може передаватися як gatekeeper, так і кінцевим обладнанням. Якщо зміна смуги пропускання неможлива, то надсилається повідомлення BRJ (Bandwidth Reject). Якщо зміна можлива, передається повідомлення BCF (Bandwidth Confirm).

Зменшення смуги пропускання можливе завжди, а для збільшення смуги пропускання понад значення, вказане в останньому повідомленні ARQ, кінцеве обладнання має закрити всі логічні канали та відкрити їх заново. Логічний канал

має бути закритий повідомленням close Logical Channel протоколу управління H.245, а відкритий з новими параметрами повідомлення Open Logical Channel.

З'єднання роз'єднується наступним чином:

- ініціатор роз'єднання повинен закрити канал повідомленням close Logical Channel, що передається каналом управління H.245;
- ініціатор роз'єднання повинен передати повідомлення end Session Command, що передається каналом управління H.245;
- віддалене обладнання чекає повідомлення end Session Command, що передається каналом управління H.245;
- якщо логічний канал сигналізації Q.931 відкрито, він закривається повідомленням Release Complete.

Якщо в системі є Gatekeeper, то він повинен звільнити раніше виділену смугу пропускання. Звільнення смуги пропускання здійснюється повідомленням DRQ (Disengage Request) сигналізації RAS, що передається кінцевим обладнанням. У відповідь має бути отримане повідомлення підтвердження DCF (Disengage Confirm) або повідомлення DRJ (Disengage Reject) відмови.

Сигналізація H.450

Додаткові послуги у мережах IP-телефонії визначає сімейство рекомендацій H.450. Так, 450.1 описує протокол сигналізації між двома компонентами мережі, що дозволяє надавати додаткові послуги, а 450.2 - механізми послуги трансформації виклику (Call Transfer), завдяки якій з'єднання між терміналами А та Б перетворюється на з'єднання між Б та В. Додаткова послуга Call Diversion, яку визначає H.450.3, надає можливість переадресувати виклик у тих випадках, коли абонент, що викликається, зайнятий, не відповідає або коли попередньо встановлено відповідний параметр.

1.3 Сигналізація на основі протоколу SIP

Протокол SIP (Session Initiation Protocol) є протоколом прикладного рівня, розробленим робочою групою управління багатоточковими сеансами мультимедіа-зв'язку (MMUSIC) організації IETF (Рекомендація RFC 2543). Він дозволяє організувати та провести такий сеанс, забезпечуючи його встановлення, модифікацію та завершення.

При організації мультимедійного сеансу використовується два основних методи знаходження та інформування зацікавлених учасників:

- повідомлення про сеанс з використанням різних засобів - електронної пошти, груп новин, Web-сторінок або спеціального протоколу SAP (Session Announcement Protocol);
- запрошення до участі у сеансі за допомогою протоколу SIP.

Для встановлення сеансів одноадресного мовлення, характерного для IP-телефонії, основним протоколом встановлення з'єднань є протокол SIP. SIP працює за схемою клієнт-сервер (рис. 1.6): клієнт запитує певний тип сервісу, а сервер обробляє його запит та забезпечує надання сервісу. Згідно з протоколом SIP, система користувача може не тільки формувати, але і приймати запити. Це означає, що вона має бути оснащена і клієнтською (клієнт агента користувача – UAC) та серверною (сервер агента користувача – UAS) частинами.

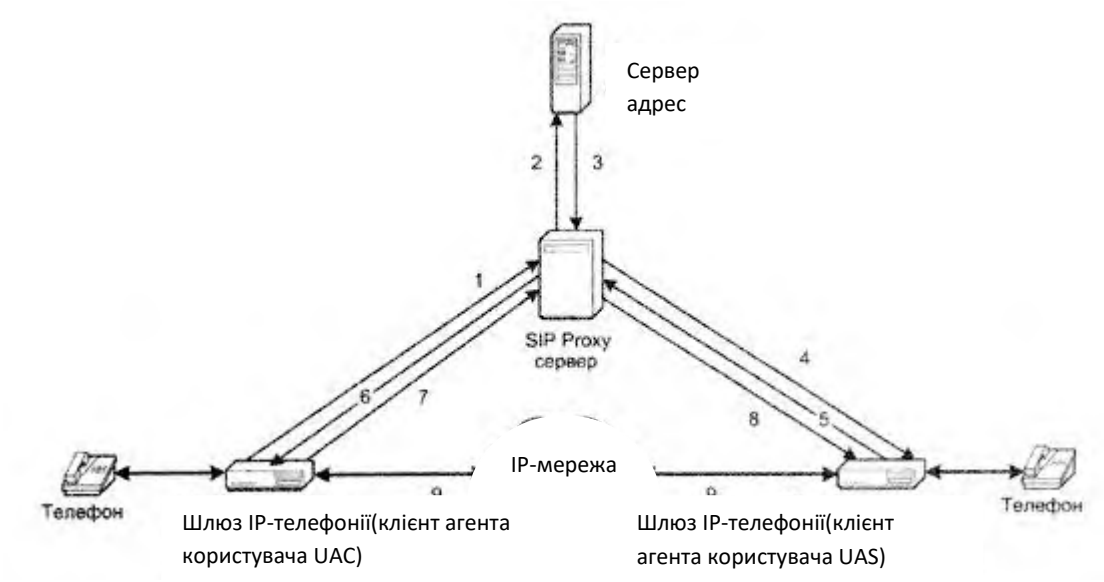


Рис. 1.6 Схема сигналізації за протоколом SIP

Здійснення викликів здійснюється сервером SIP, який може працювати в режимі безпосереднього встановлення зв'язку або в режимі переадресації. В обох режимах сервер приймає запити на визначення розташування потрібного користувача, але якщо в першому режимі він сам доводить виклик до адресата, то в другому - повертає адресу кінцевого пункту запитуваному клієнту.

У протоколі SIP визначено два види сигнальних повідомлень - запит та відповідь. Вони мають текстовий формат (кодування символів згідно з RFC 2279) і базуються на протоколі HTTP (синтаксис та семантика визначені в RFC 2068). У запиті вказуються процедури, що викликаються виконання необхідних операцій, а відповіді - результати їх виконання. Визначено шість процедур:

- INVITE – запрошує користувача взяти участь у сеансі зв'язку (служить для встановлення нового з'єднання; може містити параметри для узгодження);
- BYE – завершує з'єднання між двома користувачами;
- OPTIONS - використовується передачі інформації про підтримуваних характеристиках (ця передача може здійснюватися безпосередньо між двома агентами користувачів чи через сервер SIP);
- ACK - використовується підтвердження отримання повідомлення чи позитивного відповіді команду INVITE;

- CANCEL – припиняє пошук користувача;
- REGISTER – передає інформацію про місцезнаходження користувача на сервер SIP, який може транслювати її на сервер адрес (Location Server).

Обидва протоколи SAP та SIP використовують механізм SDP (Session Description Protocol) для опису характеристик сеансу: час проведення, необхідні ресурси тощо. (Рекомендація RFC 2327). SDP використовується виключно для текстового опису сеансу та не має ні транспортних механізмів, ні засобів узгодження необхідних для сеансу параметрів. Ці функції повинні виконувати протоколи для передачі інформації SDP.

Повідомлення-відповіді можуть містити шість типів можливих результатів: запит у процесі виконання (1xx), успішний запит (2xx), переадресація (3xx), неправильний запит (4xx), відмова сервера (5xx) та глобальна відмова (6xx). Використовується в SIP адресація заснована на уніфікованому покажчику ресурсів SIP URL, в якому може бути записано ім'я домену (user@domain) або IP-адресу (user@IPadress) користувача. Мета використання такого формату - інтеграція SIP-послуг з існуючими Інтернет-службами. Сервер імен доменів (DNS) перетворює доменні імена на IP-адреси кінцевої точки (рис. 1.7). Вся маршрутизація та передача мультимедійних потоків виконується IP-мережею, що знаходиться нижче. Таким чином, послуги SIP добре інтегруються у традиційну модель Web-комунікацій із сервером DNS, що забезпечує перетворення доменного імені на мережеву адресу.

Призначений для ініціації сеансів протокол SIP забезпечує визначення адреси користувача та встановлення з'єднання з ним. Крім цього, він є основою для застосування інших протоколів, що реалізують функції захисту, автентифікації, опису мультимедійного зв'язку і т.д. Для білінгу, наприклад, можна використовувати протокол Radius.

Прикладом реалізації протоколу SIP може бути програмна платформа eCo n vergence Server Solutions фірми Dynamicsoft, що включає такі продукти:

- SIP Proxy Server – маршрутизатор між кінцевими точками, кожна з яких визначена як UAC або UAS; на додаток до функцій забезпечення взаємодії між різними серверами платформи він надає послуги перенаправлення та реєстрації/визначення розташування користувачів;
- SIP Location Server - забезпечує безпечну сигналізацію дзвінків, зберігає інформацію про користувачів, необхідну сервіс-провайдерам для гнучкого керування доступом користувачів та маршрутизації дзвінків з метою надання найкращої якості послуги;
- SIP User Agent - керує з'єднаннями між вихідною та вхідною сторонами, забезпечуючи підтримку необхідної якості послуг;
- SIP CallAccounting Server - виконує функції збору та обробки інформації у вигляді детальних звітів про транзакції TDR, які отримують від SIP Proxy Server, яка надалі може бути використана в системах білінгу та менеджменту користувачів.

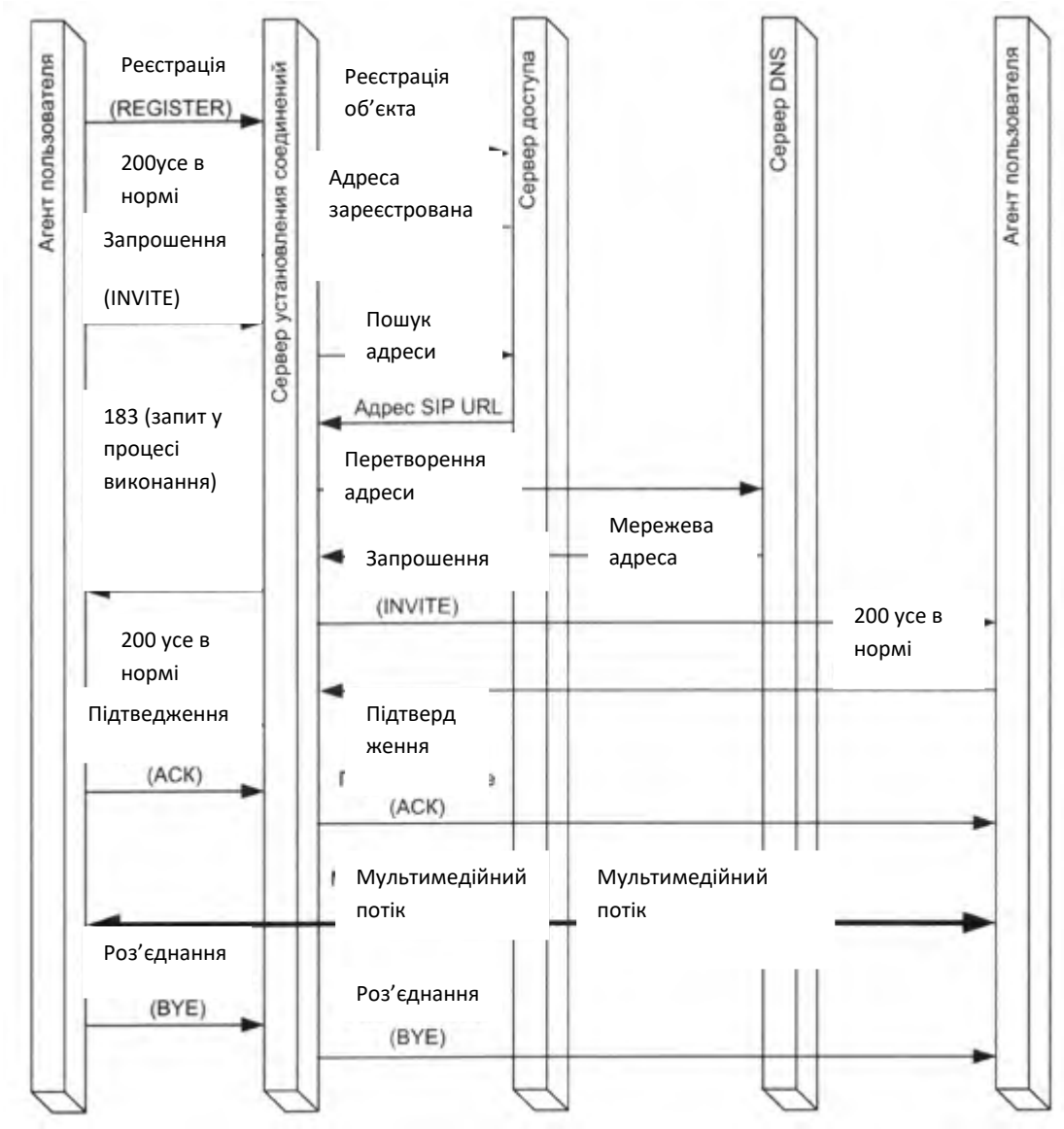


Рис.1.7 Можливий сценарій встановлення та завершення сеансу зв'язку за протоколом SIP

1.4 Порівняння протоколів H.323 та SIP

Протоколи H.323 і SIP представляють суттєво різні підходи до вирішення тих самих завдань: якщо H.323 близький до традиційних систем сигналізації (з комутацією каналів на основі протоколу Q.931 або більш ранніх рекомендацій серії H), то SIP реалізує більш простий , Інтернет підхід на основі HTTP.

Слід зазначити, що стандарт H.323 не вирішує проблеми, пов'язані із захистом виклику від несанкціонованого доступу, взаємодією між шлюзами та gatekeeper

різних мереж, між телефонами та персональними комп'ютерами, роумінгом та інтеграцією з телефонною сигналізацією ГКС №7. Протокол H.323 може лише гарантувати взаємодію типу шлюз-шлюз і телефон-телефон, оскільки орієнтований на транспортні послуги в середині мережі і не здатний щось поліпшити на рівні кінцевих вузлів. Він не передбачає будь-яких засобів, що полегшують розробку нових додатків. Алгоритми H.323 не оптимізовані для реальних мереж, вони складні в реалізації та вимагають великих ресурсів на стороні клієнта. Тим не менш, рекомендація непогано підходить для популярних сьогодні магістральних програм IP-телефонії у вигляді Інтернет-телефонії, що забезпечують суттєве зниження витрат на міжміський та міжнародний зв'язок.

У порівнянні з H.323 протокол SIP базується на текстовому форматі, більш простий для реалізації та додавання нових функцій. Протокол забезпечує реалізацію важливих систем Інтернет-телефонії функцій, включаючи шифрування і аутентифікація. Те, що SIP базується на архітектурі клієнт-сервер, дозволяє забезпечити управління викликами на рівні сервера (подібне неможливо в однорангових схемах обслуговування викликів, що використовуються більшістю кінцевих точок H.323). В даний час запропоновані специфікації, які розширюють протокол SIP засобами керування безпекою дзвінка, запиту якості обслуговування, сигналізації зміни стану мережі.

Систему об'єктів H.323 можна як прикладну мережу, накладену на мережу передачі (IP-мережа), тоді як служби SIP орієнтовані інтеграцію зі службами Інтернет. Який з варіантів кращий, залежить від необхідних функціональних можливостей .

Технологія H.323 надає більше можливостей щодо управління конкретною послугою в частині аутентифікації та обліку та контролю за використанням мережевих ресурсів. Можливості протоколу SIP тут значно менші. Вибір цього протоколу компанією-постачальником послуг фактично означає, що технологічна інтеграція послуг для неї важливіша за можливості гнучкої тарифікації та контролю за використанням мережевих ресурсів.

Загалом можна дійти невтішного висновку, що протокол SIP орієнтований на Інтернет-провайдерів, які розглядають послугу Інтернет-телефонії лише як невелику частину свого сервісного пакета. Будучи самодостатньою, технологія H.323 більше підходить для корпоративних мереж (інтранет) та постачальників послуг IP-телефонії, для яких ці послуги не є домінуючими. У цілому нині H.323 і SIP годі було розглядати як конкуруючі технології, є різними підходами, призначеними для різних сегментів ринку. Вони можуть працювати паралельно та навіть взаємодіяти через спеціальний прикордонний шлюз.

1.5 Особливості сигналізації за концепцією TIPHON

Базуючись на стандарті H.323 IP-мережі, специфікація TIPHON доповнює його деякими обов'язковими процедурами, і навіть механізмами взаємодії з мережами комутації каналів. Функціональна модель TIPHON складається з тих же компонентів -gatekeeper, шлюзу та терміналу, - що і модель H.323, проте в ній передбачено поділ шлюзу на три функціональні об'єкти. Це шлюз сигналізації (SG – Signalling Gateway), транспортний шлюз (MG – Media Gateway) та контролер транспортного шлюзу (MGC – Media Gateway Controller) (рис. 1.8).

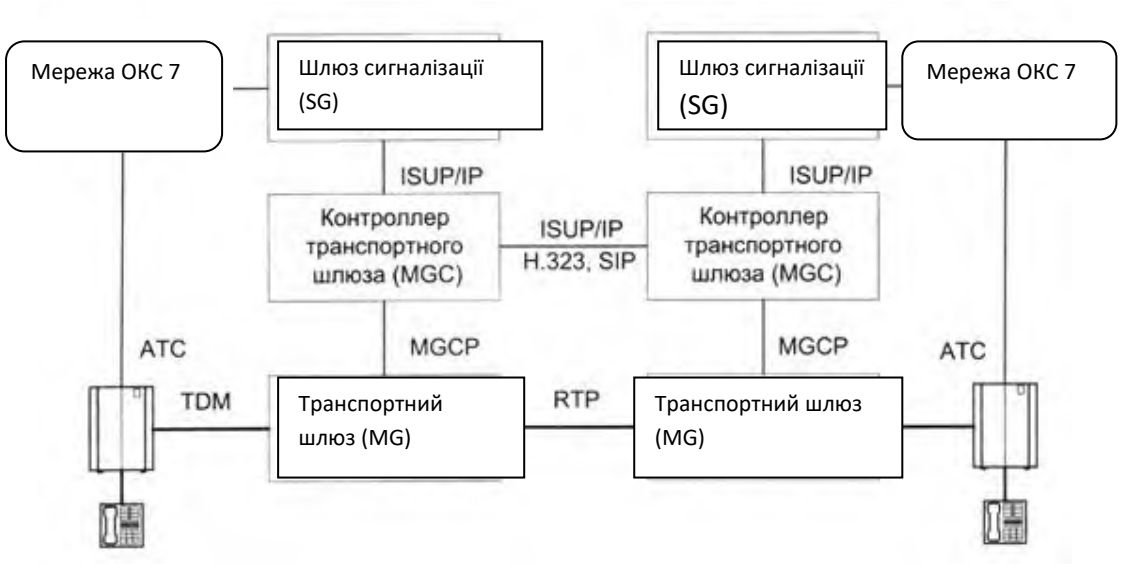


Рис. 1.8 Функціональна модель мережі за проектом TIPHON

Шлюз сигналізації служить проміжною ланкою сигналізації між мережами з пакетною і канальною комутацією. У завдання транспортного шлюзу входить

перетворення та/або перекодування інформації, що передається; він забезпечує термінування ІКМ-трафіку телефонних мереж та пакетного трафіку, транслює адреси, пригнічує відлуння, відтворює різні повідомлення для абонентів, приймає та передає цифри кодом DTMF тощо. Контролер сигналізації MGC виконує процедури сигналізації H.323, які визначені в рекомендаціях H.323, H.225 (RAS і Q.931) та H.245, і перетворює повідомлення сигналізації телефонних мереж повідомлення сигналізації H.323. Основне завдання - керувати роботою транспортного шлюзу, тобто. здійснювати контроль за сполуками, використанням ресурсів, трансляцією протоколів тощо. Слід зазначити, що MGC не забезпечує керування викликами. Це завдання gatekeeper, який виконує їх відповідно до рекомендацій H.323.

При використанні сигналізації ГКС №7 в контролер MGC по IP-мережі будуть передаватись повідомлення ISUP (підсистеми обслуговування викликів мережі ISDN). Якщо ж застосовується сигналізація по виділеному каналу (CAS), сигнальні повідомлення спочатку разом з інформацією абонента надійдуть у транспортний шлюз, а потім вже буде виділено до контролера MGC. При цьому передбачається використовувати протокол MDTP (Multi-Network Datagram Transmission Protocol), який служить для інкапсуляції телефонних протоколів сигналізації (ISUP, CAS, PRI) і передачі інформації в контролер транспортного шлюзу.

MGC аналізує інформацію сигналізації та передає керуючу інформацію в транспортний шлюз за допомогою спеціального протоколу управління, до завдань якого входить забезпечення управління різними ресурсами (системою інтерактивного мовного відгуку, мостами конференцзв'язку тощо), прийомом та формуванням сигналів DTMF, формуванням тональних сигналів (готовності до набору номера, контролю надсилання виклику, «зайнято» та ін.), луна-придушенням, використанням кодеків (G.711, G.723.1, G.729, GSM і т.д.), збором статистики, тестуванням кінцевих точок (наприклад, випробування з шлейфу), резервуванням, роз'єднанням і блокуванням кінцевих точок, шифруванням.

2 ПРОТОКОЛИ З ДЕКОМПОЗИЦІЄЮ ШЛЮЗІВ

2.1 Загальна характеристика протоколів MGCP та Megaco.

Протокол управління транспортними шлюзами MGCP є досить простим протоколом клієнт-сервер. Логіка управління викликами виконується агентом (Call Agent), що знаходиться поза транспортним шлюзом. Сам транспортний шлюз представляється у вигляді об'єкта, що складається з кінцевих точок - точок входу/виходу інформаційних потоків і з'єднань - двох або більше з'єднаних кінцевих точок. Модель визначає фізичні кінцеві точки (наприклад, закінчення з'єднувальних ліній) та віртуальні кінцеві точки (наприклад, аудіо джерела). Сам протокол MGCP використовує принцип «провідний/відомий», згідно з яким агент управління викликами передає транспортному шлюзу команди для керування кінцевими точками та з'єднаннями, а також ініціації певних дій. MGCP є досить універсальним протоколом, здатним забезпечити розподілене керування різними типами транспортних шлюзів, зокрема телефонними шлюзами та серверами доступу. Він може використовуватися для встановлення з'єднання та виконання різних функцій обслуговування, наприклад, тестування шлейфу.

Подальшим розвитком протоколу MGCP є протокол управління викликами Megaco (Media Gateway Control), відомий також як стандарт ITU H.248, який визначає взаємодію, з одного боку, шлюзу між різними середовищами передачі даних (Media Gateway, MG) та, з іншого, - контролера шлюзів між середовищами передачі (Media Gateway Controller, MGC) (рис. 2.1). Іншими словами, Megaco розроблено для внутрішньо-доменного віддаленого керування пристроями, що відповідають за встановлення з'єднання або проведення сеансу зв'язку, включаючи шлюзи VoIP, сервери віддаленого доступу, мультиплексори цифрових абонентських ліній (DSL), маршрутизатори з підтримкою багатопротокольної комутації. використанням міток (Multiprotocol Label Switching, MPLS), оптичні крос-конектори, модулі агрегування сеансів PPP та інші.

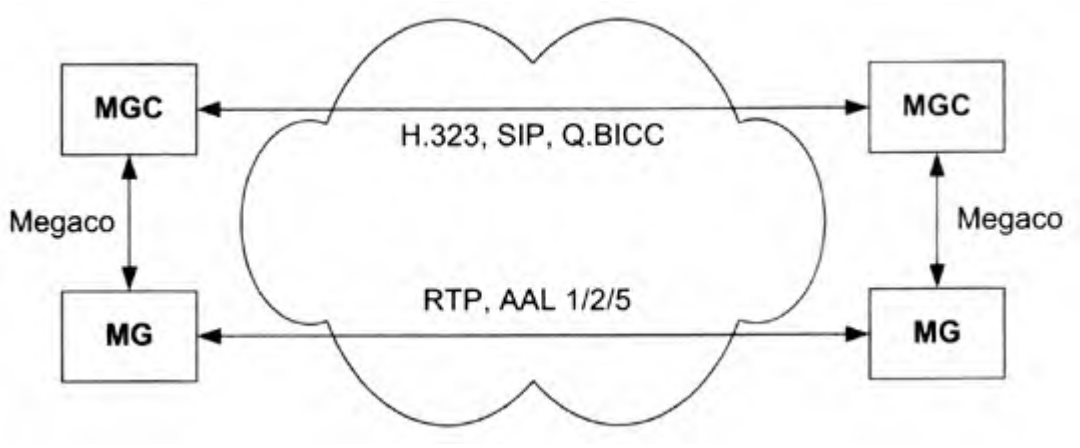


Рис. 2.1 Використання протоколу Megaco у мережі IP-телефонії

MGCP і Megaco - ці порівняно низькорівневі протоколи управління пристроями, які повідомляють шлюзу, яким чином зв'язати потоки, що надходять до мережі з комутацією пакетів або осередків, з потоками пакетів або осередків, що переносяться, наприклад, транспортним протоколом реального часу (Real-Time Transport Protocol, RTF). По суті, Megaco повторює MGCP щодо архітектури та взаємодії контролера зі шлюзом, але при цьому Megaco підтримує ширший діапазон мережевих технологій, у тому числі ATM.

2.2 Протокол MGCP.

2.2.1 Архітектура мережі за протоколом MGCP.

При розробці протоколу MGCP робоча група MEGACO спиралася на принцип декомпозиції, за яким шлюз розбивається окремі функціональні блоки (рис. 2.2.):

• транспортний шлюз - Media Gateway , який виконує функції перетворення мовної інформації, що надходить з боку ТФОП з постійною швидкістю, у вигляд, придатний для передачі мережами з маршрутизацією пакетів IP : кодування та упаковку мовної інформації в пакети RTP / UDP / IP , а також зворотне перетворення;

• пристрій керування - Call Agent , що виконує функції керування шлюзом;

• шлюз сигналізації - Signaling Gateway , який забезпечує доставку сигнальної інформації, що надходить з боку ТФОП, до пристрою керування шлюзом та перенесення сигнальної інформації у зворотному напрямку.

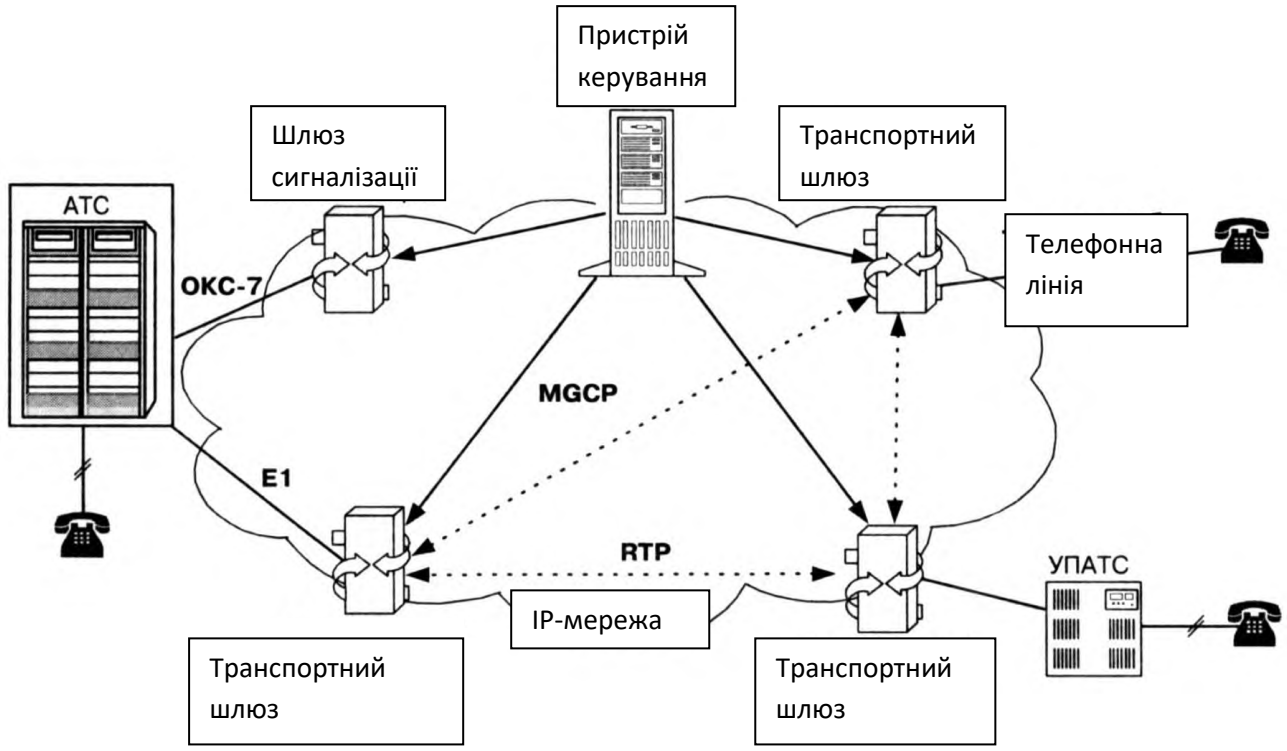


Рис. 2.2 Архітектура мережі, що базується на протоколі MGCP

Таким чином, весь інтелект функціонально розподіленого шлюзу розміщується у пристрої керування, функції якого, у свою чергу, можуть бути розподілені між кількома комп'ютерними платформами. Шлюз сигналізації виконує функції STP - транзитного пункту системи сигналізації загальним каналом - ОКС7. Транспортні шлюзи виконують лише функції перетворення мовної інформації. Один пристрій керування обслуговує одночасно кілька шлюзів. У мережі може бути кілька пристроїв керування.

2.2.2 Встановлення, зміна та руйнування з'єднань.

Розглянемо, яким чином за допомогою протоколу MGCP встановлюються, змінюються та завершуються мовні з'єднання у мережах з маршрутизацією пакетів IP . Приклад охоплює взаємодію протоколу MGCP з протоколом ОКС7 (рис. 2.3).

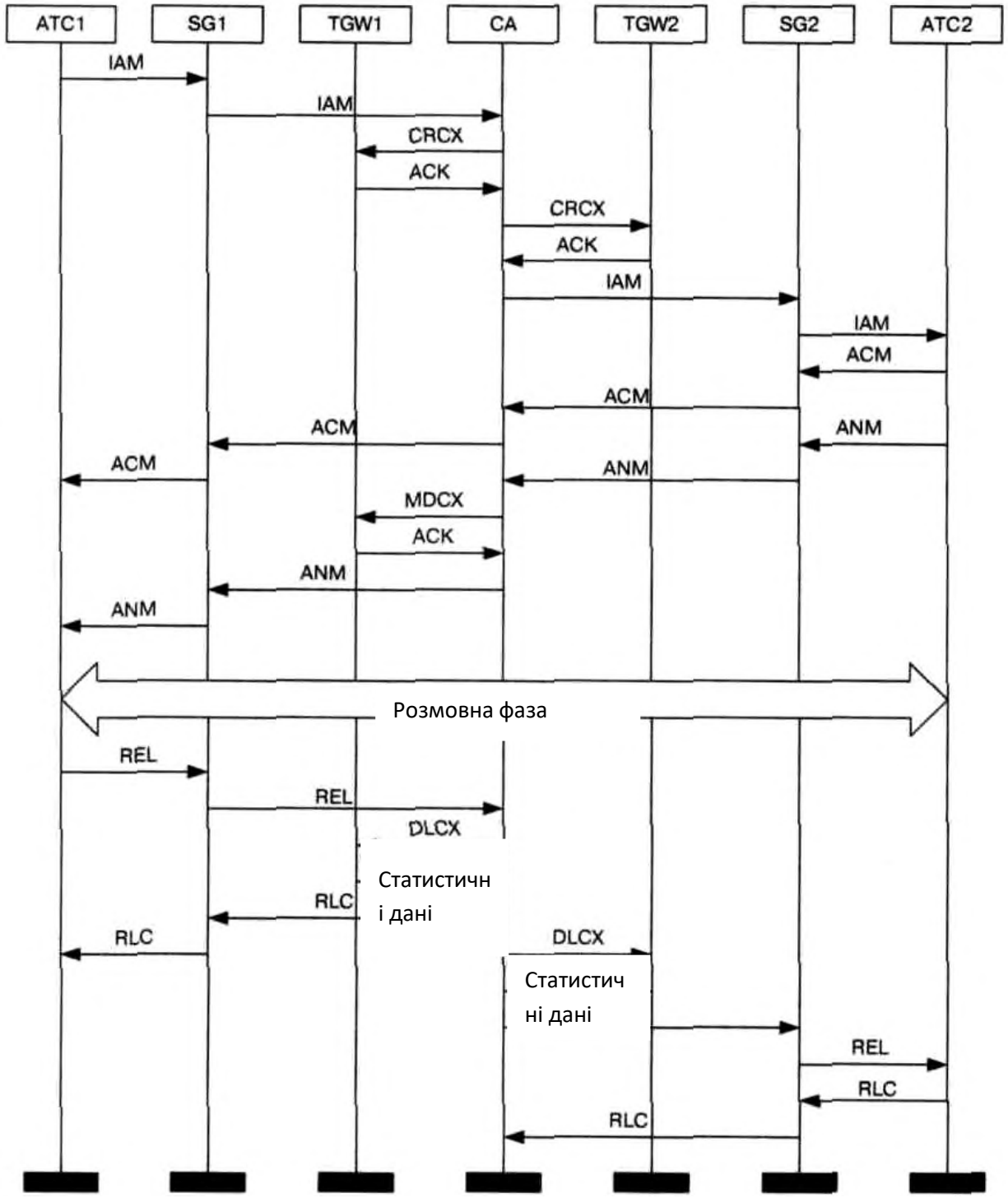


Рис. 2.3 Встановлення та руйнування з'єднання з використанням протоколу MGCP

Від телефонної станції АТС1 до шлюзу сигналізації SG 1 загальному каналу сигналізації надходить запит з'єднання - повідомлення IAM . Шлюз SG1 передає повідомлення IAM пристрою керування шлюзами Call Agent , яке обробляє запит і визначає, що дзвінок має бути направлений до телефонної станції АТС2 за допомогою шлюзу TGW 2.

Далі Call Agent резервує порт шлюзу TGW 1 (розмовний канал). З цією метою Call Agent передає шлюзу команду Create Connection (створити з'єднання) - CRCX . Зазначимо, що порт шлюзу TGW1 може лише приймати інформацію (режим « recvonly -шлюзу слід тільки приймати»), оскільки він ще не обізнаний про те, на яку адресу і яким чином слід передавати інформацію.

У відповіді АСК прийняту команду шлюз TGW1 підтверджує опис сеансу зв'язку.

Після прийому від шлюзу TGW 1 підтвердження Call Agent передає команду CRCX другому шлюзу TGW 2 з метою зарезервувати в ньому порт:

Шлюз TGW 2 вибирає порт, який братиме участь у зв'язку, та підтверджує прийом команди CRCX повідомленням АСК.

За допомогою двох команд CRCX створюється односпрямований розмовний канал для передачі абоненту, що викликається, акустичних сигналів або мовних підказок і повідомлень. У той же час, порт шлюзу TGW 2 вже може не тільки приймати, а й передавати інформацію, оскільки він отримав опис сеансу зв'язку зустрічного шлюзу. Далі Call Agent передає повідомлення I AM (запит на з'єднання) до телефонної станції АТС2. На повідомлення I AM станція АТС2 відповідає повідомленням ACM(згода на встановлення з'єднання), яке негайно пересилається до станції АТС1.

Після того як абонент прийме виклик, телефонна станція АТС2 передає до Call Agent повідомлення ANM (дзвінок прийнято) Далі Call Agent змінює режим з'єднання recvonly в шлюзі TGW 1 на повнодуплексний режим, команда MDCX-змінити параметри з'єднання.

Шлюз TGW1 виконує та підтверджує зміну режиму з'єднання повідомленням АСК.

Call Agent передає повідомлення ANM (виклик прийнято) до телефонної станції АТС1, після чого настає розмовна фаза з'єднання.

Завершення розмовної фази відбувається в такий спосіб. У нашому випадку абонент дає відбій першим, телефонна станція АТС1 через шлюз сигналізації передає до Call Agent повідомлення REL (завершення розмови). На підставі цього повідомлення Call Agent завершує з'єднання з абонентом, передаючи повідомлення DLCX (завершення з'єднання).

Шлюз підтверджує завершення з'єднання та передає до Call Agent зібрані за час з'єднання статистичні дані:

Далі Call Agent передає до АТС1 повідомлення RLC з метою підтвердження руйнування з'єднання.Паралельно Call Agent завершує з'єднання з викликаною стороною: Шлюз TGW 2 підтверджує завершення з'єднання та передає до Call Agent зібрані під час з'єднання статистичні дані.

Після отримання відповіді на команду DLCX Call Agent може розпочинати процедуру завершення з'єднання з АТС2, яка має підтвердити роз'єднання, після чого з'єднання вважається зруйнованим.

2.3 Протокол MEGACO.

2.3.1 Архітектура мережі за протоколом MEGACO.

Як видно з малюнку 2.4, архітектура мережі, що базується на використанні протоколу MEGACO, за своїми функціональними властивостями аналогічна архітектурі мережі з використанням протоколу MGCP .

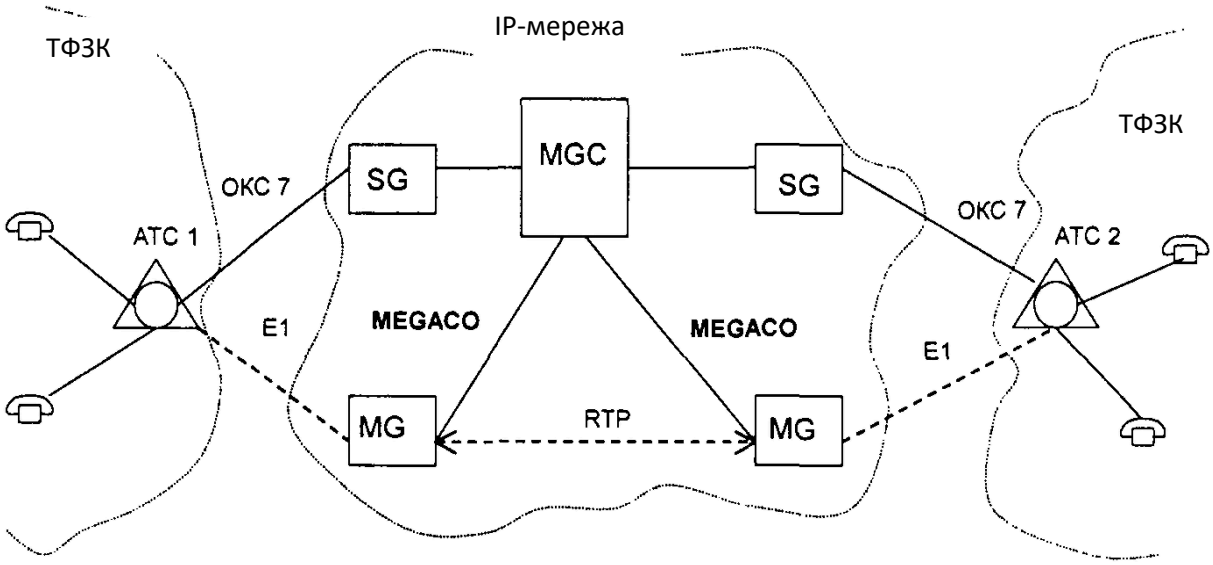


Рис.2.4 Архітектура мережі за допомогою протоколу MEGACO.

Однак, система команд і сценарій встановлення та руйнування з'єднання з використанням протоколу Megaco має деяку відмінність від протоколу MGCP

2.3.2 Приклад встановлення та руйнування з'єднання за протоколом MEGACO.

Розглянемо коротко основні особливості протоколу MEGACO/H.248. Для передачі 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, як і, як і технології ATM, є необов'язковою.

На малюнку 2.5 наведено приклад встановлення з'єднання з використанням протоколу MEGACO між двома шлюзами (Residential Gateway), керованими одним контролером.

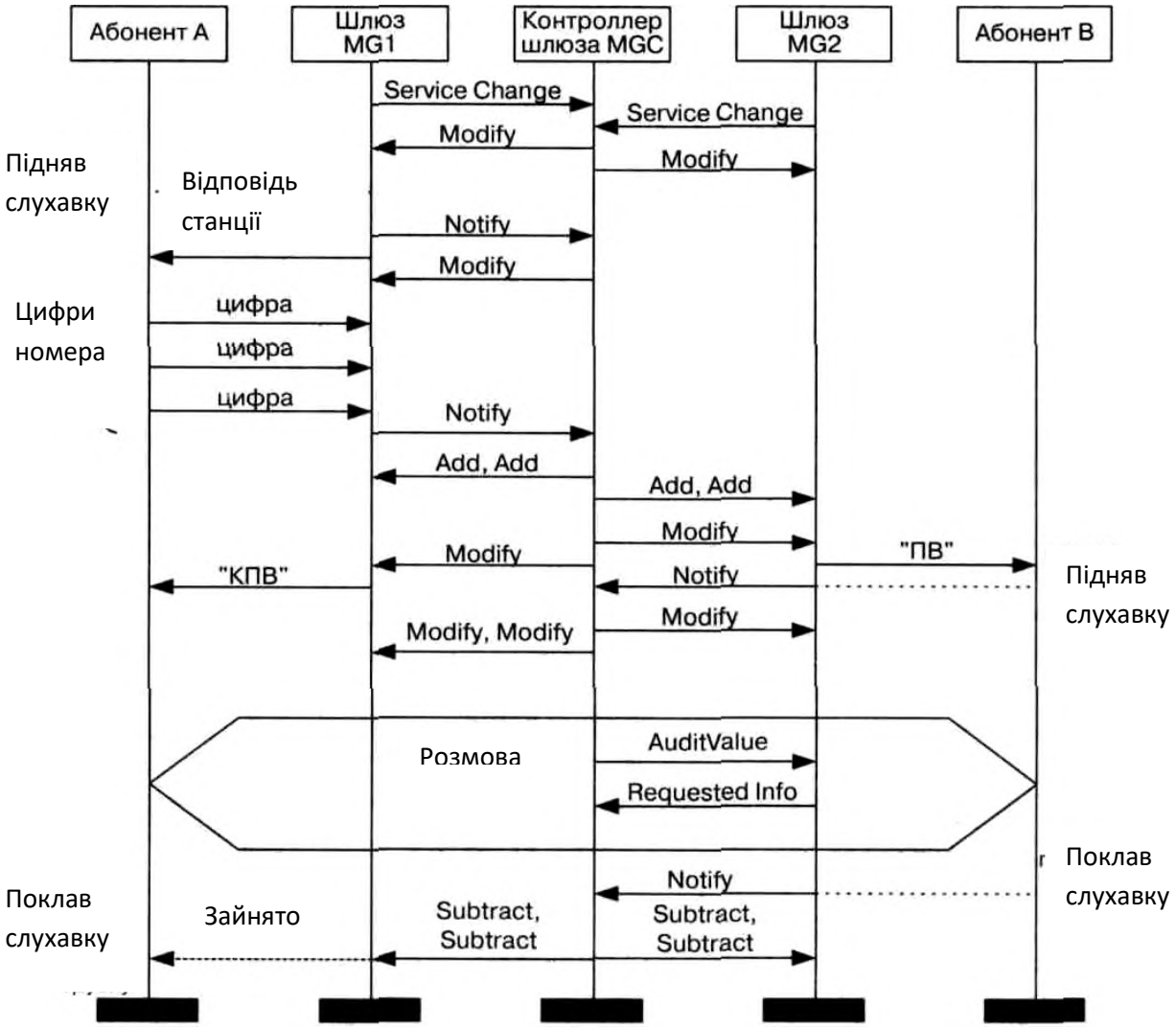


Рис. 2.5 Алгоритм встановлення та руйнування з'єднання за допомогою протоколу MEGACO

Таблиця 2.1

Команди протоколу MEGACO/H.248

Команда	Напрямок передачі	Призначення
Add (Додати)	MGC -> MG	Контролер дає вказівку шлюзу додати порт до контексту
Modify (Змінити)	MGC -> MG	Контролер дає вказівку шлюзу змінити властивості порту
Subtract (Вимкнути)	MGC -> MG	Контролер вилучає порт із контексту
Move (Перекласти)	MGC -> MG	Контролер переводить порт з одного контексту до іншого в одну дію
AuditValue (Перевірити порт)	MGC -> MG	Контролер запитує властивості порту, події або сигнали, що відбулися, що передаються в канал, а також статистику, зібрану на поточний момент часу
AuditCapabilities (Перевірити можливості порту)	MGC -> MG	Контролер запитує можливі значення властивостей порту, перелік подій, які можуть бути виявлені портом, перелік сигналів, які порт може посилати в канал, статичні дані
Notify (Повідомити)	MG -> MGC	Шлюз інформує контролер про події, що відбулися.
ServiceChange (Рестарт)	MG -> MGC, MGC -> MG	Шлюз інформує контролер про те, що один або кілька портів виходять із робочого стану або повертаються до робочого стану. Контролер може наказати порту або групі портів вийти з обслуговування або повернутися в обслуговування

1. Шлюз MG1 реєструється у контролера MGC за допомогою команди ServiceChange. Використання нульового контексту означає, що порт зараз не бере участі в жодному з'єднанні, а використання ідентифікатора порту ROOT означає, що команда відноситься до всього шлюзу, а не до якогось певного порту.

2. Контролер підтверджує реєстрацію шлюзу.

3. Шлюз має вільні аналогові порти, які мають бути запрограмовані для відстеження зміни опору абонентського шлейфу, що означає підняття абонентом трубки, після чого шлюз повинен передати абоненту акустичний сигнал «Відповідь станції». Програмування провадиться за допомогою команди Modify з відповідними параметрами, причому програмується порт, що знаходиться в нульовому контексті. У команді вказується ідентифікатор порту (terminationid)-A4444, ідентифікатор інформаційного потоку (streamid)-1, транспортна адреса обладнання, що передала команду -55555, специфікується режим функціонування -дуплексний (SendReceive).

На цьому етапі в шлюз може бути завантажений план нумерації (у дескрипторі digit map). У цьому випадку, після того, як абонент підніме трубку, шлюз повинен передати йому акустичний сигнал «Відповідь станції» та розпочинати прийом сигналів DTMF відповідно до плану нумерації. Однак у нашому прикладі план нумерації буде завантажений лише після того, як абонент підніме слухавку на 8 кроці.

Крім того, слід зазначити, що кроки 3 і 4 даного алгоритму можуть бути поєднані з кроками 8 і 9 відповідно за допомогою дескриптора EventsDescriptor. При цьому кроки 6 та 7 опускаються.

4. Шлюз MG1 підтверджує виконання команди Modify.

5. Подібним чином (кроки 1-4) програмується аналоговий порт шлюзу MG2, в нашому прикладі має ідентифікатор A5555.

6. Далі шлюз MG1 виявляє, що абонент А підняв трубку, і повідомляє про цю подію Media Gateway Controller за допомогою команди Notify.

7. Контролер підтверджує отримання команди Notify .

8. На наступному кроці MGC дає шлюзу інструкцію накопичувати цифри номера абонента відповідно до обраного плану нумерації. Крім того, після отримання

першої цифри номера необхідно зупинити передачу акустичного сигналу "Відповідь станції".

9. Шлюз підтверджує одержання команди Modify.

10. Цифри номера абонента, що викликається, збираються шлюзом MG1, після чого вони порівнюються з планом номерації і передаються контролеру.

11. Отримане повідомлення підтверджується контролером.

12. Далі контролер MGC аналізує цифри номера абонента, отриманого від шлюзу MG1, і визначає, що з'єднання має проходити через шлюз MG2, до якого підключений абонент, що викликається.

13. Шлюз MG1 створює новий віртуальний порт і вказує його віртуальну адресу.

14. Контролер MGC створює в шлюзі MG2 контекст для встановлення дуплексного з'єднання (режим Send Receive) з користувачем, що викликає.

15. Створення контексту підтверджується, що фізичний порт шлюзу MG2 A5555 з'єднується з UDP/RTP портом, що має ідентифікатор A5556. Зазначимо, що RTP-порт має номер 1111, тобто. відмінний від номера порту Megaco/H.248 – 55555.

16. Контролер MGC наказує порту A5555 шлюзу MG2 почати передачу викликного сигналу.

17. Шлюз MG2 підтверджує передачу сигналу «Здійснення виклику» абоненту, що викликається.

18. Контролер наказує шлюзу MG1 почати передачу абоненту, що викликає, акустичного сигналу «Контроль здійснення виклику (КПВ)».

19. Шлюз MG1 підтверджує передачу зазначеного акустичного сигналу порт A4444.

На цьому етапі обом абонентам, що беруть участь у з'єднанні, надсилаються відповідні сигнали, і шлюз MG2 чекає, поки абонент, що викликається, прийме вхідний виклик, після чого між двома шлюзами будуть організовані двонаправлені розмовні канали.

20. Шлюз MG2 виявив, що абонент підняв трубку, і повідомляє про це контролер MGC.

21. Контролер підтверджує отримання команди Notify.

22. Далі контролер MGC наказує шлюзу MG2 припинити передачу викликного сигналу.

23. Шлюз MG2 підтверджує виконання команди.

24. Далі, контролер дозволяє шлюзу MG1 не тільки приймати, але й передавати інформацію (режим SendReceive), і зупиняє передачу абоненту акустичного сигналу «КПВ».

25. Шлюз MG1 підтверджує виконання команди.

26. Після цього починається розмовна фаза з'єднання, протягом якої учасники обмінюються мовленнєвою інформацією. Наступним кроком контролер MGC вирішує перевірити PTP-порт у шлюзі MG2.

27. Шлюз MG2 виконує команду. У відповіді на команду AuditValue передається вся інформація, що запитується, у тому числі статистика, зібрана за час з'єднання. Крім того, з відповіді видно, що не відбулося жодних подій та не передавалося жодних сигналів.

28. абонент першим завершує з'єднання, і шлюз MG2 сповіщає про це контролер MGC.

29. Контролер MGC підтверджує отримання повідомлення Notify.

30. Отримавши інформацію від будь-якого зі шлюзів про те, що один із абонентів поклав трубку, контролер MGC завершує з'єднання. До обох шлюзів передається команда Subtract. Алгоритм завершення з'єднання передбачає однаковий обмін сигнальними повідомленнями між контролером та обома шлюзами, тому цей алгоритм розглядається на прикладі шлюзу MG2.

31. Кожен із портів шлюзу MG2, що беруть участь у з'єднанні (фізичний порт - A5555 та RTP-порт - A5556), повертає статистику, зібрану за час з'єднання. У випадку, контролер може запитувати статистичну інформацію лише в одного з портів.

32. Після завершення з'єднання контролер MGC наказує шлюзам MG1 і MG2 бути готовими до того, що хтось із абонентів, які вони обслуговують, підніме трубку. Примітно, що портам шлюзу, які відображаються закінченнями в нульовому контексті, за замовчуванням може бути наказано виявляти, що абонент підняв трубку, при цьому контролер не передає шлюзам спеціальні команди, як це було показано раніше (крок 3).

Протоколи MGCP і Megaco дуже схожі один на одного, і для багатьох додатків немає значення, який з них буде використовуватися. Однак Megaco краще інтегрований з додатками з підтримкою кількох середовищ передачі, ніж MGCP, тому що базовий протокол включені семантичні елементи для конференцій. Завдяки цьому MGCP може бути найкращою основою для програм, не прив'язаних до будь-якого середовища, наприклад, для управління сеансами на базі MPLS.

2.4 Міжмережева взаємодія

При впровадженні систем IP-телефонії часто потрібно вирішувати завдання забезпечення ефективної взаємодії мереж різних операторів. Тут існує безліч проблем, пов'язаних із перетворенням адрес між адміністративними доменами, взаєморозрахунками між операторами, контролем доступу до ресурсів мережі, захистом внутрішньої топології і т.д. Успішне вирішення даних завдань має забезпечувати відповідну систему сигналізації IP-телефонії.

У третій версії рекомендацій H.323 з'явився додаток G до H.225. У ньому описаний метод взаємодії адміністративних доменів за допомогою об'єкта, що називається прикордонним елементом (Border Element). Цей функціональний елемент підтримує відкритий доступ до адміністративного домену для доведення дзвінка до вузла, що входить до цього домену, або надання інших послуг, що вимагають встановлення мультимедіа зв'язку з його вузлами.

Взаємодія між прикордонними елементами здійснюється через протокол, визначений у додатку G. Він може бути використаний з метою обміну планами

нумерації та тарифікаційною інформацією, відомостями для авторизації та маршрутизації викликів, звітами про використання мережевих ресурсів.

Подібні функції міжмережевої взаємодії реалізовані у проекті TIPHON. На рис. 2.6 показаний приклад передачі сигнальної інформації між терміналом та шлюзом, розташованими у різних адміністративних доменах.



Рис.2.6 Приклад взаємодії двох доменів

У сценарії, показаному на рис. 2.7, ресурси зони H.323 (термінал, шлюз і сервер авторизації), необхідні реалізації виклику IP-телефонії, розділені між трьома адміністративними доменами. У даному випадку два домени (перший і другий) не мають встановлених сигнальних відносин, але кожен повинен мати сигнальні відносини з третім доменом, в якому розташований центр авторизації. На рис. 2.7. показані такі потоки інформації:

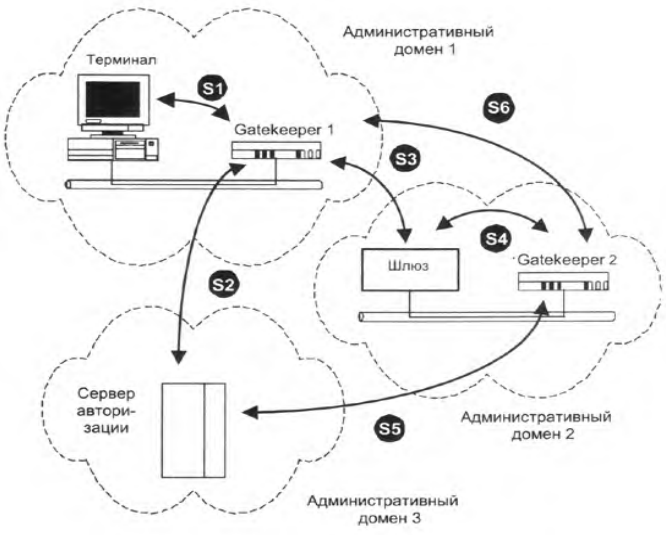


Рис. 2.7 Приклад взаємодії трьох доменів

S1: Обмін інформацією дозволу запиту між терміналом і gatekeeper 1.

S2: Обмін інформацією дозволу запиту між gatekeeper 1 та сервером авторизації.

S3: Обмін інформацією дозволу запиту між gatekeeper 1 та шлюзом.

S4: Обмін інформацією дозволу запиту між шлюзом та його gatekeeper.

S5: Обмін інформацією дозволу запиту між gatekeeper 2 і сервером від третьої особи.

S6: Обмін інформацією дозволу запиту між gatekeeper 1 та gatekeeper 2.

Слід зазначити, що реалізація передачі сигнальної інформації між різними адміністративними доменами в мережі IP-телефонії вимагає забезпечення відповідного ступеня захисту інформації.

Таким чином, розвиток систем I P-телефонії пов'язаний, головним чином, з удосконаленням протоколів сигналізації. Основна складність, що виникає при цьому, обумовлена типом мереж між якими встановлюється сеанс IP-телефонії: ТФОП, TCP/IP, ISDN та інші. Протокол SIGTRAN призначений для того, щоб зменшити вплив цієї проблеми. Однак, найбільш повно це завдання вирішується за допомогою програмного комутатора S OF TSWITCH .

2.5 Порівняльний аналіз протоколів MGCP та MEGACO

Почнемо із загальних характеристик протоколів.

Обидва протоколи використовуються в мережах з однаковою архітектурою, де керують транспортними шлюзами високоінтелектуальні контролери. Обидва протоколи вміють працювати зі шлюзами тих самих видів, класифікація шлюзів була дана в попередньому розділі. Порти шлюзів підтримують детектування тих самих подій і генерацію тих самих сигналів. Використовуються однакові транспортні механізми доставки повідомлень систем сигналізації ОКС7, DSS1, ТСК. Процедури встановлення та руйнування з'єднань, що реалізуються обома протоколами, ідентичні. Крім того, використовуються однакові механізми

підтримки захисту мережі. На цьому подібність протоколів MGCP та MEGACO/H.248 закінчується.

Найважливішою відмінністю протоколу MEGACO/H.248 від протоколу MGCP є використання іншої моделі зв'язку. Протокол MEGACO/H.248 працює не лише з телефонними портами, а й з UDP-портами. Крім того, connection у моделі MGCP - це, в загальному випадку, підключення до з'єднання між портами різного обладнання, у той час як context у моделі MEGACO/H.248 завжди відображає зв'язок між портами одного шлюзу (рис. 2.8).

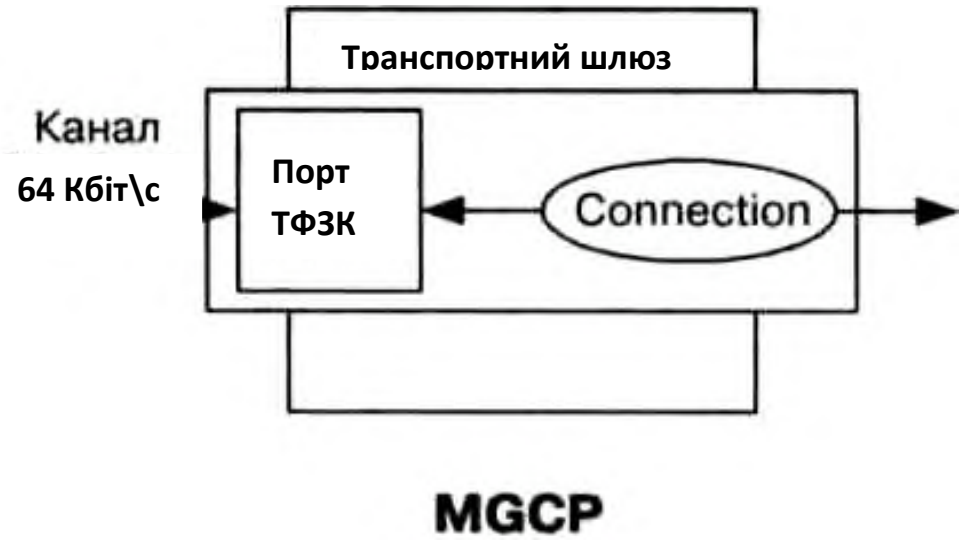


Рис.2.8 Модель MGCP.

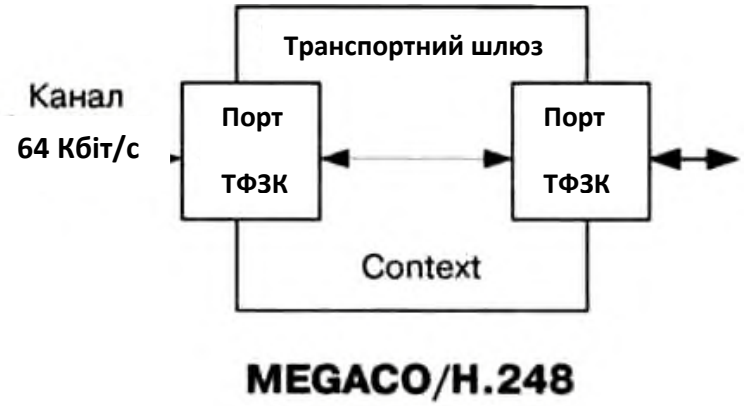


Рис. 2.9 Модель MEGACO/H.248

Змінюючи топологію зв'язків портів, що належать до одного контексту, за допомогою протоколу MEGACO контролер може гнучко керувати конференціями. Даної можливості у протоколі MGCP не передбачено.

Вище зазначалося, що з протоколу MEGACO/H.248 передбачено два способи кодування, тоді як повідомлення протоколу MGCP представляються у текстовому форматі, а бінарний спосіб кодування не підтримується. Крім того, у протоколах використовуються різні параметри команд та коди помилок.

Протокол MEGACO/H.248, як і протокол MGCP, передбачає кореляцію команд і відповідей. Але якщо в протоколі MGCP транзакція утворюється з команди та відповіді на неї, то в протоколі MEGACO/H.248 транзакція складається із запиту - сукупності акцій та відгуку на запит. Загальна структура запиту виглядає так :

TransactionRequest(Transactionid {

ContextiD {Command ... Command),

ContextiD (Command ... Command } })

Загальна структура відгуку на запит наведена нижче:

TransactionReply(TransactionID {

ContextiD { Response ... Response },

ContextiD { Response ... Response } })

Кожна акція, у свою чергу, складається з однієї або кількох команд, що належать до одного контексту, та відповіді на них (Рис. 2.10). Використання такого інструменту дозволяє значно зменшити обсяг сигнальної інформації, що передається, і збільшити швидкість встановлення з'єднань за рахунок того, що контролер може паралельно вести обробку сигнальної інформації, що відноситься до різних з'єднань.

Аналоги двох надлишкових команд EndpointConfiguration і Notifica-tionRequest протоколу MGCP у протоколі MEGACO/H.248 відсутні, але водночас додана команда Move, що дозволяє в одну дію перевести порт з одного контексту в інший. Як приклад використання команди Move наведемо сценарій додаткових послуг «Повідомлення про вхідний виклик та переведення існуючого з'єднання в режим утримання», англомовна назва послуг - Call Waiting та Call Hold.

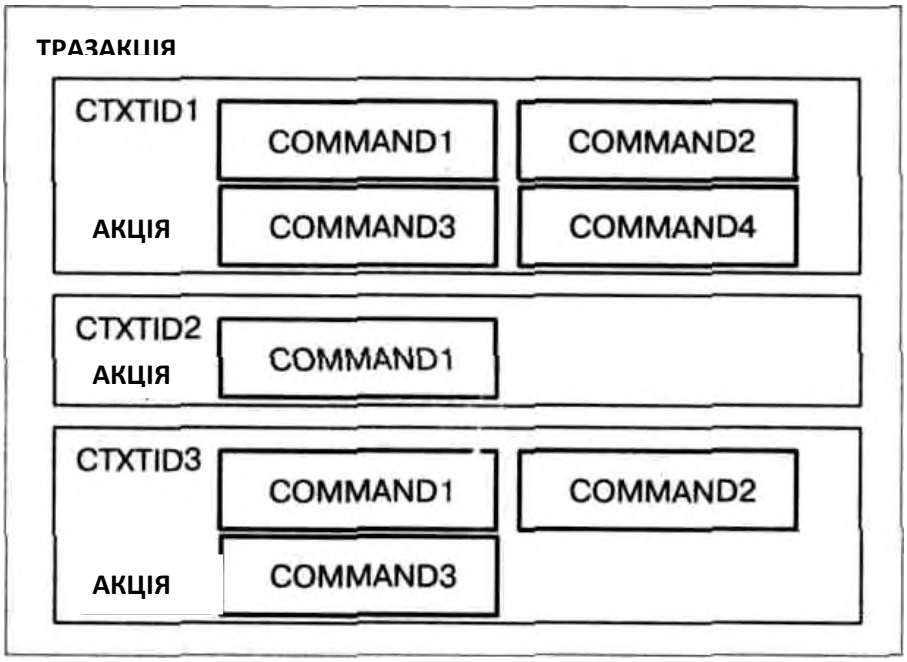


Рис. 2.10 Транзакція протоколу MEGACO/H.248

Абонент А розмовляє з абонентом В, а абонент С викликає абонента А, при цьому абоненту, що викликається, передається акустичне повідомлення про вхідний виклик (рис. 2.11). Далі абонент А переводить з'єднання з абонентом У режим утримання і з'єднується з абонентом З (рис.2.11). Реалізація комбінації додаткових послуг Call Waiting та Call Hold, тобто. передача порту з одного контексту в інший стала можливою завдяки команді Move.

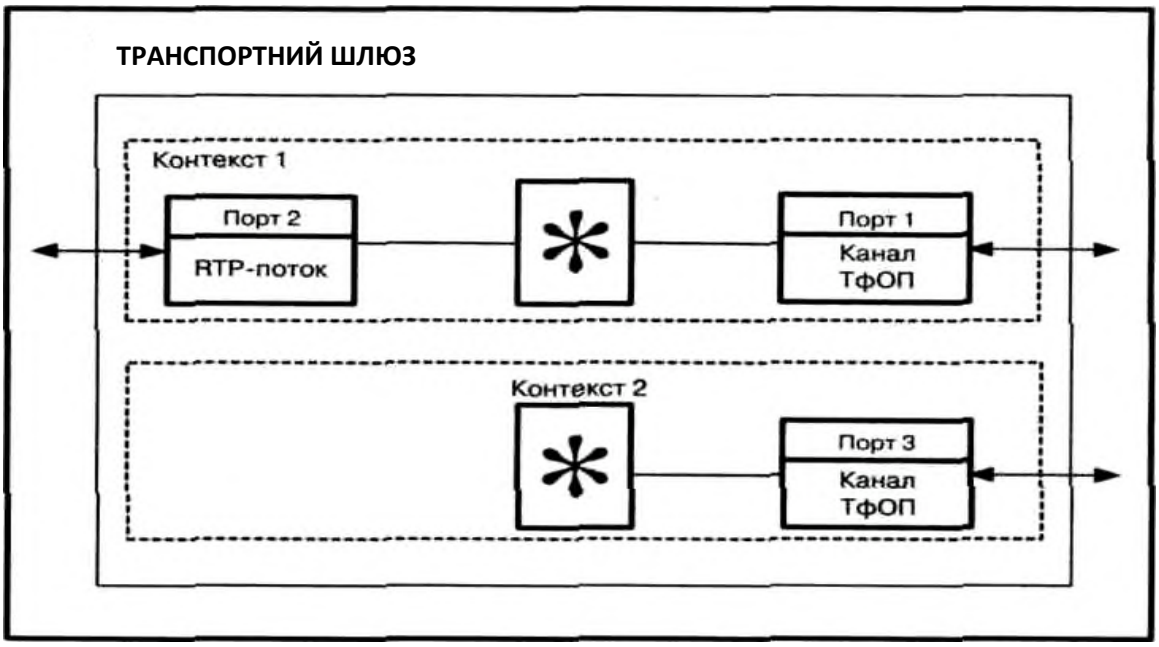


Рис. 2.11 Сценарій реалізації послуги Call Waiting

На закінчення даного параграфа хотілося б відзначити, що невідомо, коли знадобиться розширена, в порівнянні з MGCP, функціональність протоколу MEGACO/H.248. Крім того, на базі протоколу MGCP побудовано низку мереж IP-телефонії. Все це означає, що обидва протоколи MGCP і MEGACO/H.248 можуть спільно використовуватися в одній мережі.

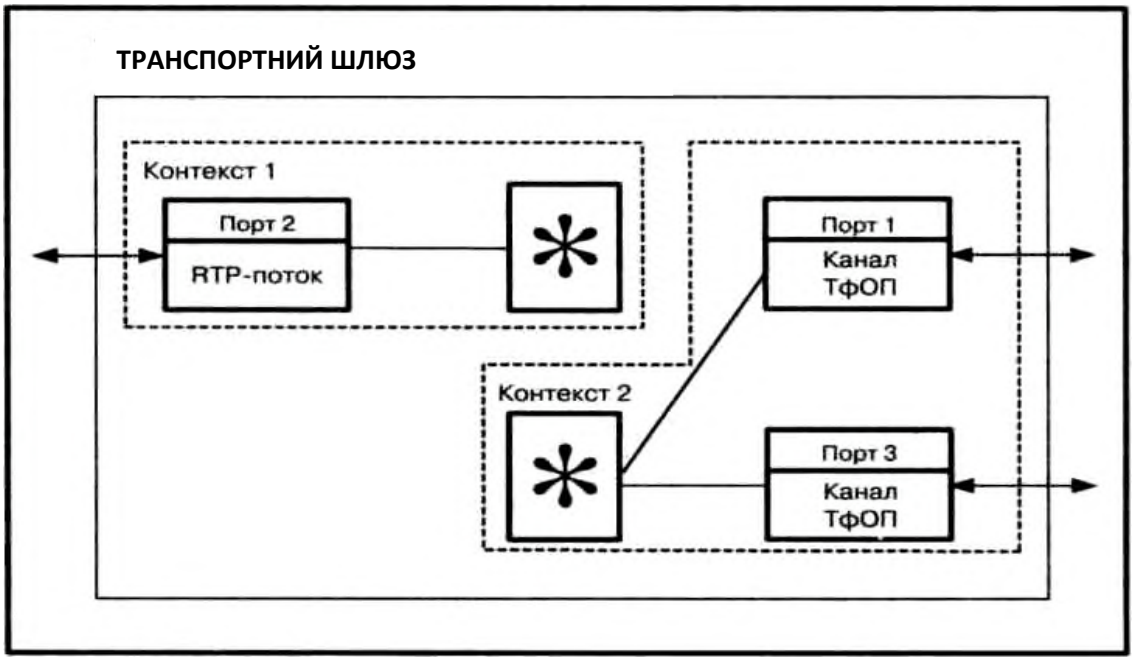


Рис. 2.12 Сценарій реалізації послуги Call Hold

3 АРХІТЕКТУРА SIGTRAN

3.1 Рівні моделі Sigtran у стеку протоколів TCP / IP

Архітектура Sigtran , визначена RFC 2719, передбачає такі рівні:

- стандартний протокол IP ,
- загальне транспортування сигналів, що забезпечує доставку повідомлень без помилок і в належному порядку, незалежно від капрізів мережі IP , що знаходиться нижче, за протоколом *SCTP [Stream Control Transmission Protocol).*
- рівень адаптації, що забезпечує інтерфейс з протоколами та додатками верхнього рівня, так що ці програми не відчувають, що нижчележаче транспортування здійснюється в IP -середовищі, а не за традиційними протоколами перенесення повідомлень MTP стека ОКС 7 , наприклад .

Зауважимо відразу, що протокол SCTP надає можливість використовувати його для надійної доставки сигнального трафіку інших типів, що не входить у стек О КС 7. В область інтересів Sigtran включені також адаптаційні рівні різних протоколів, що дає можливість пересилати по SCTP сигнальні повідомлення не тільки ОКС 7 , наприклад, Q .931 ISDN або V 5.2. Архітектура Sigtran детально показана на рис. 3.1. У цій архітектурі, завдяки - пересиланню незалежних послідовностей повідомлень в окремих потоках SCTP (що обговорюється нижче в цьому параграфі), гарантується вільна від помилок доставка повідомлень з дотриманням черговості їх прямування, забезпечується швидка доставка повідомлень і зменшується вплив повторної передачі втраченого повідомлення на своєчасність доставки повідомлень з інших послідовностей за рахунок так званого *блокування з відносним пріоритетом { head - of ~ line blocking),* що робить SCTP більш відповідним протоколом, ніж TCP .

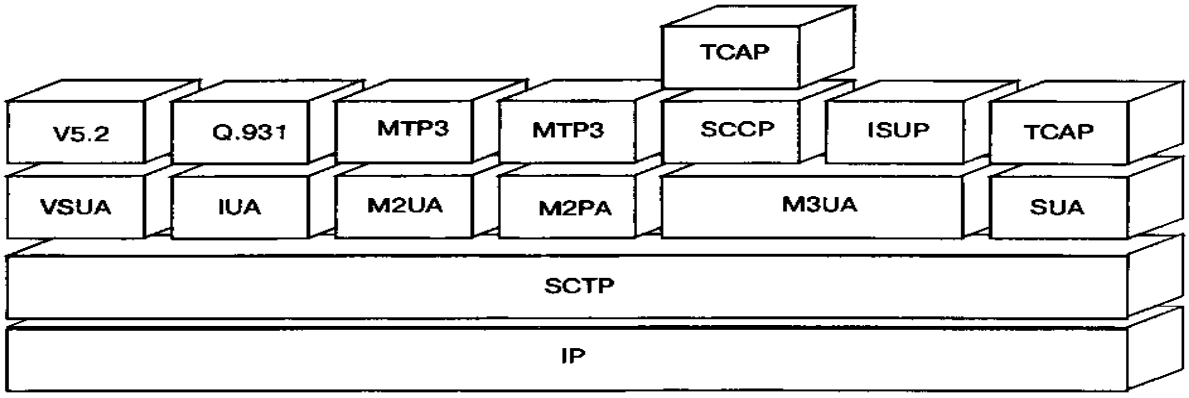


Рис. 3.1 Архітектура протоколу Sigtran .

Протокол SCTP розглядається у наступному параграфі. Після цього описуються рівні адаптації, які забезпечують сполучення SCTP з протоколами верхнього рівня. Більшість із них орієнтовано на ОКС 7, в першу чергу, на протокол ISUP , але два відносяться до сигналізації інших типів.

3.2 Адаптаційні рівні Sigtran .

До числа модулів адаптації, що працюють поверх SCTP , входять такі.

M2UA (MTP2-User Adaptation Layer) забезпечує адаптацію SCTP до MTP 3 таким чином, щоб стандартний протокол MTP 3 міг використовуватися в мережі IP , реалізуючи транспортування повідомлень через SCTP та IP замість MTP 2. Наприклад, реалізований в Softswitch стандартний додаток MTP 3 може обмінюватися керуючими повідомленнями мережної сигналізації із зовнішньою мережею ОКС 7. Так само, як у мережі ОКС 7 MTP 2 надає свої послуги MTP 3, M 2 UA надає свої послуги MTP 3 у мережі IR M 2 UA має номер порту 2904.

M2PA (MTP2 Peer-to-PeerAdaptation Layer) також забезпечує адаптацію SCTP до MTP 3, але вже в іншій області. Аналогічно випадок з M 2 UA , рівень MTP 3 у вузлі мережі IP (Softswitch , зокрема) обмінюється інформацією з M 2 PA , ніби він був звичайним MTP 2. Відмінності між M 2 UA і M 2 PA визначаються їх ролями в мережевий архітектурі: якщо Softswitch з'єднується з мережею ОКС 7 просто на правах терміналу

сигналізації ОКС 7, достатньо застосування М 2 UA . Шлюз SG , який використовує М 2 РА , сам фактично є транзитним пунктом сигналізації SIP на базі IP , у нього є власний код пункту сигналізації, він може також виконувати функції сигналізації верхнього рівня, такі як функції SCCP .

М 3 UA { MTP 3- User Adaptation Layer) забезпечує інтерфейс між SCTP і тими протоколами ОКС 7, які використовують послуги МТР 3, наприклад, ISUP і SCCR Завдяки М 3 UA ці протоколи не відчувають, що замість типового транспортування МТР 3 використовується транспортування SCTP поверх IP . Однак М 3 UA - просто адаптаційний рівень між протоколами верхнього рівня і SCTR , він не є повною копією МТР 3 в IP -мережі і не реалізує деякі стандартні керуючі повідомлення мережевої сигналізації МТР 3, такі як TFA , TFP та ін.

SUA { SCCP - User Adaptation Layer забезпечує інтерфейс між протоколом SCCP стека ОКС 7 і SCTR завдяки чому такі прикладні підсистеми-користувачі SCCP як TCAP використовують послуги SUA точно так, як вони використовують послуги SCCP в мережі ОКС 7, навіть не підозрюючи, що все це відбувається в IP -мережі.

IUA (ISDN Q .921- User Adaptation Layer) теж працює поверх SCTP і забезпечує для сигналізації DSS 1 за рекомендацією Q .931 прозоре транспортування повідомлень по мережі I P точно так, як вони передаються рівнем ланки даних Q .921 мережі ISDN .

V 5 UA { V 5.2- UserAdaptation Layer) має ряд схожих з протоколом IUA характеристик і може розглядатися як розширення IUA , його Sigtran- версія розглядається нижче.

3.3 Транспортний протокол із керуванням потоками SCTP

3.3.1 Основні функціональні можливості SCTP

Протокол передачі з керуванням потоками SCTP (Stream Control Transmission Protocol) специфікований в документі RFC 2960 і є протоколом сімейства IP за номером 132. Підставою для його розробки послужила вже нездатність, що вже обговорювалася вище, як UDP , так і TCP забезпечити швидкість і надійність, необхідні для транспортування сигнальних повідомлень протоколів верхнього рівня, званих *Upper - layer Protocol (UPL),* які не вимагають повного набору функціональних можливостей протоколу TCP , але продовжують віддавати перевагу орієнтованому на з'єднання протоколу транспортного рівня зі збереженням даних про стани. Ці завдання має вирішити SCTP . За змістом протокол SCTP аналогічний TCP , але він удосконалить операції перенесення даних, збереження даних про стани та оновлення цих даних щодо тих дій, які необхідні для надійного та стійкого транспортування потоків повідомлень UPL між портами. У зв'язку з цим у протоколі SCTP , що пропонується на зміну TCP , реалізуються наступні принципи:

- достовірне, вільне від помилок і не дубльоване пересилання даних у *потоках повідомлень (message streams),* при якій усувається необхідність у забезпеченні суворого порядку проходження повідомлень, та повідомлення пересилаються на вищележачий рівень, як тільки вони отримані;
- сегментація даних для адаптації до розміру максимального блоку даних, що пересилається, що, втім, є обов'язковою умовою в світі IP і передбачає складання блоків даних у повідомлення на дальньому кінці;
- відсутність обов'язкового мультиплексування повідомлень у SCTP - дейтаграми;
- відмовостійкість на мережному рівні;

- виключення перевантажень та протидія лавинам повідомлень та нелегальним проникненням у систему, що викликає перевантаження ;
- функції експлуатаційного керування трактом передачі, що дозволяють встановити доступність адресата в режимі реального часу за допомогою періодичних контрольних повідомлень, і якщо виявляється, що поточна транспортна адреса одержувача недоступна, вибирається інша адреса зі списку можливих транспортних адрес цього одержувача.

Незважаючи на те, що протокол SCTP є орієнтованим на з'єднання в тому сенсі, що порти терміналів встановлюють між собою з'єднання перед тим, як почати передачу даних, він, порівняно з протоколом TCP , є в деяких сферах застосування більш простим (причому не через надійності та стійкості транспортного рівня), проте в інших областях таким не є. Він використовує деякі з алгоритмів, які були розроблені в останні роки, а також накопичений досвід оптимального використання пропускної спроможності для максимального підвищення продуктивності протоколу TCP у глобальних та високошвидкісних локальних обчислювальних мережах. Розглянемо основні терміни протоколу SCTP .

3.3.2 Множинна адресація

Кінцевий пункт SCTP являє собою логічний передавач або приймач пакетів SCTP і являє собою комбінацію однієї або декількох адрес і номера порту, причому SCTP дозволяє кінцевому пункту мати декілька IP -адрес і бути, таким чином, *multihomed* - розподіленим по декількох фізичних - платформах, - забезпечуючи тим найбільш стійкість до ушкоджень. Навіть маючи кілька IP -адрес, кінцевий пункт SCTP може використовувати лише один номер порту. Таким чином, якщо у кінцевого пункту кілька IP -адрес, до кожного з них застосовується один і той же номер порту SCTP .

Комбінація IP -адреси та номера порту називається *транспортною - адресою одержувача (Active Destination), що* використовується передаючим портом для повідомлень користувача. Якщо активна транспортна адреса недоступна, інші адреси віддаленого порту пробуються зі списку можливих

транспортних адрес. Зауважимо, що будь-яка транспортна адреса може застосовуватися тільки до одного кінцевого пункту SCTP , хоча кінцевий пункт може мати декілька транспортних адрес.

SCTP працює шляхом встановлення зв'язків між кінцевими пунктами SCTP . Такий зв'язок називають *асоціацією* або, менш точно, але більш звично, - *з'єднанням,* причому воно визначається учасниками, що беруть участь у ньому, кінцевими пунктами SCTP і поточним станом протоколу. Т.ч., *SCTP - з'єднання [SCTPassociation)* - це протокольний зв'язок між двома SCTP - портами, що містить протокольну інформацію про стан, включаючи теги верифікації та активний в даний момент набір порядкових номерів передачі TSN . Два SCTP -порти в будь-який момент часу не повинні мати між собою більше одного SCTP- з'єднання. Перш ніж додатки двох віконних пунктів зможуть обмінюватися інформацією, необхідно встановити з'єднання. Коли комунікацію закінчено, з'єднання можна припинити. Зауважимо, що протоколи верхнього рівня ISUP , SCCP , TCAP та ін. не обізнані про такі з'єднання, більше того, вони не виявляють того факту, що сигнальні повідомлення переносяться не стандартною MTp а чимось іншим.

Множинна адресація дозволяє встановлювати з'єднання між двома кінцевими пунктами через кілька адрес IP і/або мережевих інтерфейсів. Приклад множинної адресації SCTP показано на рис. 3.2, де обидва кінцеві пункти А і мають два інтерфейсу для SCTP -соединений. Ці кінцеві пункти мають канали двох типів: супутниковий у верхній частині малюнка та ATM у нижній частині. Одна з адрес визначена як основна, а інша може використовуватися як резервна при відмові основної адреси або у випадку, якщо програма верхнього рівня вимагає використовувати виключно резервну адресу.

Вбудована підтримка протоколом SCTP кінцевих пунктів з множинною адресацією особливо корисна в середовищі, яке потребує високої доступності додатків, як у разі транспортування сигналів ОКС 7. З'єднання SCTP з множинною адресацією може також прискорювати відновлення після відмов каналу без переривання поточного пересилання даних.

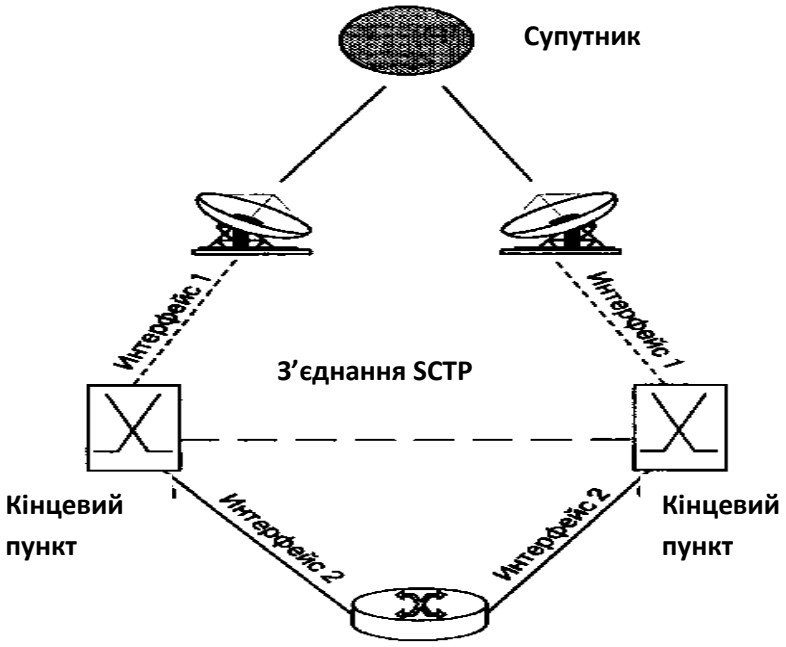


Рис. 3.2 З'єднання SCTP для кінцевих пунктів із множинною адресацією

3.3.3 З'єднання для кількох потоків

Коли встановлюється з'єднання між кінцевими пунктами, потрібно враховувати кількість потоків, які це з'єднання має підтримувати.

Наочно це з'єднання можна уявити як односторонню автомобільну - магістраль між кінцевими пунктами, то окремі потоки, які воно підтримує, будуть аналогічні окремим смугам руху на цій магістралі.

Повертаючись від цієї наочної аналогії до практичного застосування принципу, наведемо рис. 3.3, що ілюструє можливість

мультиплексувати дані програми верхнього рівня в одному з'єднанні SCTP

.

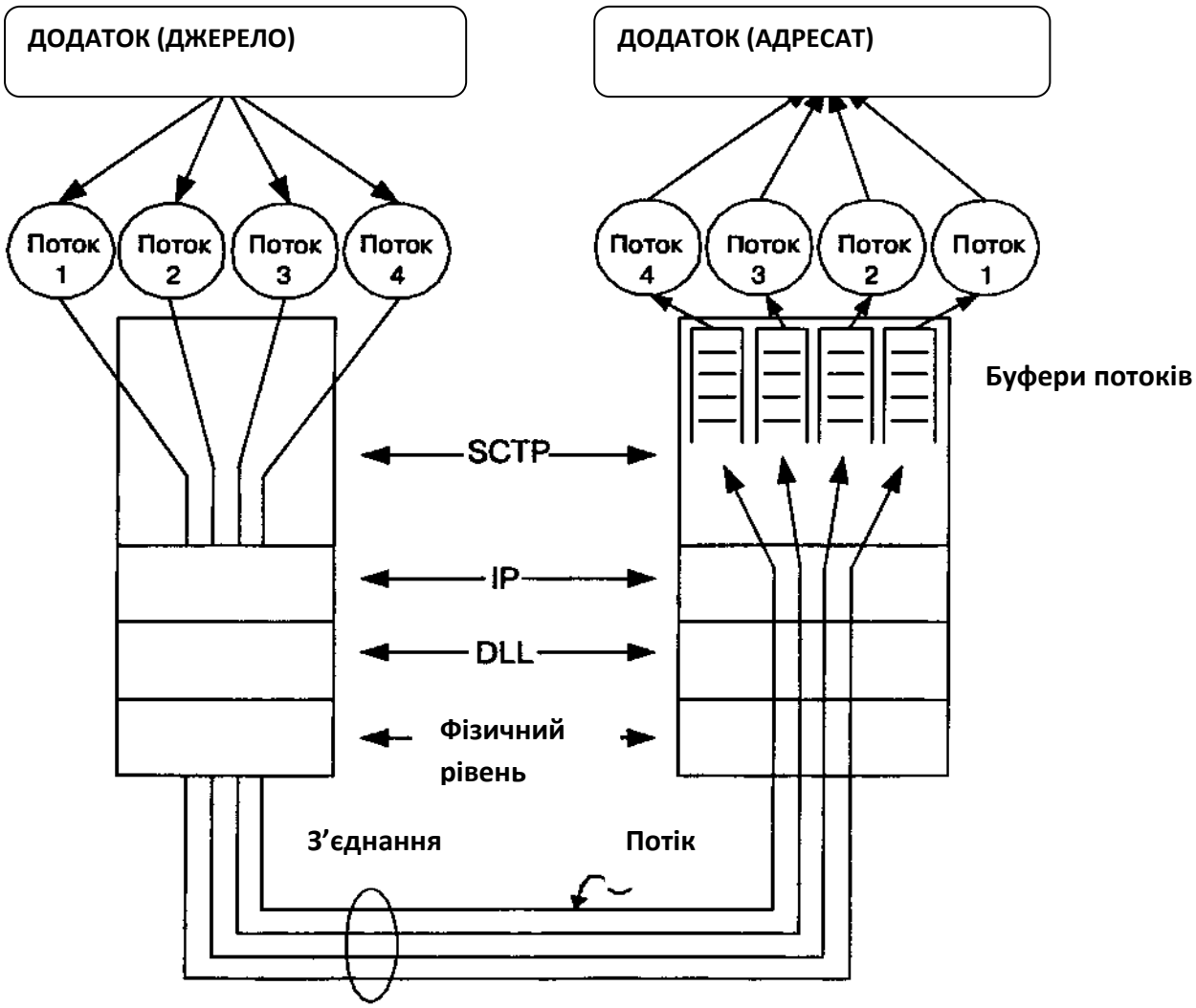


Рис. 3.3 SCTP -з'єднання для чотирьох потоків даних однієї програми

У кожному потоці виконується впорядкування даних. Якщо фрагмент пакета, що належить деякому потоку, втрачено, то фрагменти цього пакета, що йдуть за втраченим, будуть зберігатися в буфері приймача потоку, поки втрачений фрагмент не буде переданий джерелом повторно. Однак фрагменти пакетів з інших потоків можуть, як і раніше, проходити додаток верхнього рівня. Цим виключається блокування *head - of - line* , що має місце в TCP , де дані з усіх додатків верхнього рівня пересилаються в одному потоці. Інакше кажучи, ефект блокування *head - of - line* обмежений межами окремих потоків, але не проявляється для з'єднання в цілому. Простіше

кажучи, кожен потік обробляється окремо, так що доставка повідомлень одного потоку не затримується через очікування наступного повідомлення повідомлення іншого потоку.

На закінчення нагадаємо, що з передачі *з спілкування користувача (user message),* одержуваного від протоколу верхнього рівня ULP , SCTP передає IP так званий пакет SCTP , а той маршрутизує його до місця призначення. Пакет SCTP складається із загального заголовка та декількох фрагментів (chunks), як показано на рис. 3.4.

3.3.4 Фрагменти

Фрагмент (chunk - невеликий шматок) - це частина інформації всередині SCTP -пакета, що складається з заголовка і вмісту, що висить від програми. Загальний заголовок SCTP -пакету на рис.3.4. включає номери портів джерела і пункту призначення, які в поєднанні з IP -адресами джерела і пункту призначення однозначно визначають кінцеві пункти. Далі до складу заголовка входить тег верифікації, який використовується для підтвердження даних про відправника пакета. Тег верифікації ще буде описаний у цьому розділі докладніше.

Загальний заголовок містить контрольну суму Adler -32, яка утворюється особливим підрахунком значень всіх октетів пакета. Ця контрольна сума служить для того, щоб гарантувати відсутність пошкоджень в отриманому пакеті, і забезпечує ще один рівень захисту на додаток до контрольної суми заголовка IP .

За загальним заголовком йдуть кілька фрагментів. Кожен фрагмент містить свій заголовок плюс деякий вміст. Цей вміст може бути або керуючою інформацією SCTR або інформацією користувача SCTR У разі користувальницької інформації SCTP з ULP значення ідентифікатора ID.

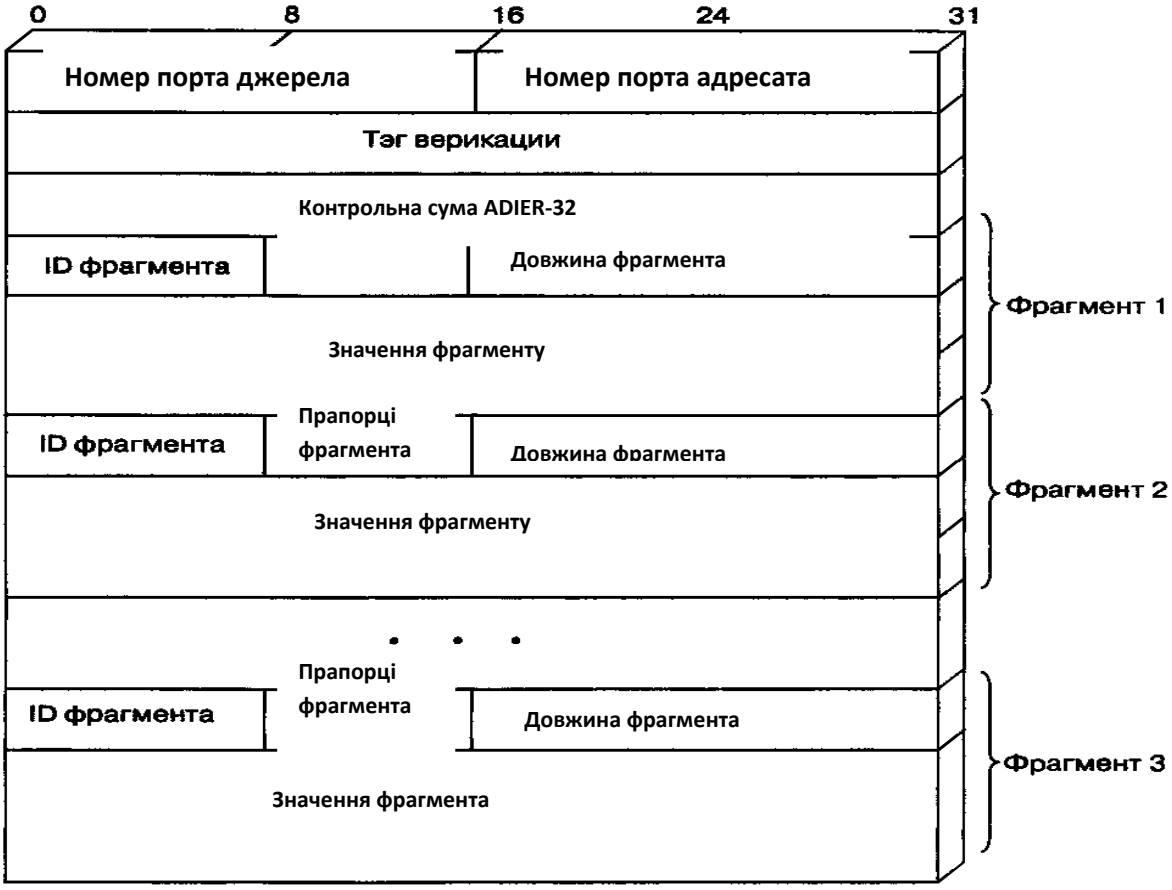
Рис. 3.4 Формат пакету SCTP

В іншому випадку ідентифікатор фрагмента матиме

Довжина фрагмента

значення , що вказує тип керуючої інформації SCTP . Можливі значення прапорів та довжини залежать від ідентифікатора фрагмента.

Хоча всього може бути до 256 різних ідентифікаторів фрагмента , існують чотири основні їх категорії: ідентифікатори перенесення даних користувача SCTP , ідентифікатори перенесення керуючої інформації SCTP , ідентифікатори, які -



резервовані IETF , і ідентифікатори перенесення розширень, визначених . Типи фрагментів описуються у табл. 3.

Таблиця 3.1

Фрагменти пакетів протоколу SCTP

Ім'я фрагмента	Опис застосування
DATA (0)	Фрагменти зданими портами терміналів, що передаються, після того, як між ними встановлено SCTP -з'єднання. Щоб забезпечити ранню передачу даних, фрагменти DATA можуть об'єднуватися в фуппи з керуючими фрагментами COOKIE - ECHO і COOKIE - ACK , поки керуючі фрагменти йдуть у повідомленні першими. Повідомлення можуть сегментуватися, щоб не перевищувався за даний максимальний розмір переданого блоку інформації MTU . Якщо це має місце, прапор фрагмента вказує початок і кінець сегмента вихідного повідомлення. Фрагменти DATA можуть доставлятися в порядку їх прийому (і тоді вони можуть бути невпорядкованими), або перед доставкою повідомлення до протоколу верхнього рівня може проводитися повна збірка вихідного повідомлення. Тип обслуговування, що запитується потоком, вказується прапором фрагмента_____
INIT(1)	Це перший фрагмент, який ініціює встановлення SCTP – со – єднання між двома терміналами. Він переносить такі параметри, як транспортна адреса з'єднання (може бути більше однієї адреси і може бути адреса протоколу IPv4, IPv6 або їх поєднання), кількість вхідних потоків, яку може підтримувати відправник, і кількість вихідних потоків, які бажає підтримувати відправник в даному SCTP- з'єднанні . Тут же віддаленому порту повідомляється про резервування ресурсів відправником (розмір вхідного буфера в байтах)
INITACK{2)	Підтверджує прийом фрагмента INIT і містить змінну стану cookie . Може також ідентифікувати непізнані параметри в повідомленні INIT і, подібно до INIT , задає кількість вихідних і вхідних потоків для SCTP - з'єднання з портом терміналу, а також транспортні адреси, які можуть використовуватися в цьому з'єднанні _____

Продовження таблиці 3.1

SACK (3)	Підтверджує отримання фрагментів DATA або інформує про те, що в послідовності прийнятих фрагментів DATA є розрив _____
HEARTBEAT REQUEST (4)	Передається періодично для підтвердження доступності порту одержувача_____
HEARTBEAT ACK (5)	Підтверджує запит HEARTBEAT ACK . Повинен передаватися на вихідну IP - адресу відправника фрагмента HEARTBEAT REQUEST
ABORT (6)	Негайно закриває з'єднання SCTP і може містити параметри, які вказують причину
SHUTDCWN (7)	Передається, щоб ініціювати поступове закриття SCTP-з'єднання
SHUTDOWN ACK(8)	Отримувач повідомлення SHUTDOWN передає це повідомлення як підтвердження
ERROR (9)	Вказує різні несправності порту. Помилки можуть бути внутрішніми або помилками протоколу, такими як некоректні параметри при керуванні фрагментами DATA
COOKIEECHO{10)	Використовується тільки у фазі встановлення SCTP - з'єднання і завершує процес встановлення з'єднання у _____ відправника даних.
COOKIE-ACK(11)	Підтверджує отримання COOKIE - ECHO у фазі встановлення SCTP з'єднання. Може об'єднуватися в групу з фрагментом DATA , але повинен бути першим фрагментом у такому зв'язуванні _____
ECNE{12)MCWR (13) _____	Повідомлення про явне навантаження та зменшене вікно навантаження, резервовані для майбутнього використання
SHUTDOWN C0MPLETE(14)	Підтверджує отримання SHUTDOWN ACK

Значення ID фрагментів кодуються двома старшими бітами, що визначають дію, яку потрібно виконати у випадку, якщо обробний пункт не дізнається тип фрагмента. Можливі значення цих бітів та їх зміст:

- **00** - зупинити обробку цього пакета SCTP та відкинути його; інші фрагменти у цьому пакеті не обробляти;
- **01** - зупинити обробку цього пакета SCTP та відкинути його; решта фрагментів у цьому пакеті не обробляти. Надіслати повідомлення про невідомий параметр Unrecognized Parameter Type (у фрагменті ERROR або INITACK);
- **10** - пропустити цей фрагмент та продовжити обробку;
- **11** - пропустити цей фрагмент і продовжити обробку, але надіслати повідомлення у фрагменті ERROR з використанням Unrecognized Parameter Type як причина помилки.

Фрагмент INIT використовується для ініціювання з'єднання SCTP між двома кінцевими пунктами. На відміну від багатьох інших, фрагмент INIT не повинен ділити пакет SCTP з іншими фрагментами . Інакше кажучи, пакет БСТР, що містить фрагмент INIT , не повинен містити жодних інших фрагментів.

Фрагмент INIT ACK використовується для підтвердження ініціювання - з'єднання SCTP . Як і фрагмент INIT , фрагмент INITACK не повинен ділити пакет SCTP з іншими фрагментами.

Фрагмент SACK служить для підтвердження прийому фрагментів DATA (корисного навантаження) та повідомлення відправника про перепустки у послідовності прийнятих фрагментів. Не кожен прийнятий фрагмент заслуговує на передачі у відповіді фрагмента SACK . Фрагмент SACK працює як покажчик місця пропуску. Припустимо, що приймач отримав фрагменти з 1 по 5, а також фрагменти 8 і 9 Повідомлення SACK інформує про відсутність фрагментів 6 і 7. Потрібно повторно передати тільки ці фрагменти. Такий метод ефективніший за механізм повторної передачі в TCP.

Фрагмент HEARTBEAT використовується для перевірки досяжності певного кінцевого пункту. Припустимо, що протягом якого відрізка часу ніякі фрагменти передавати з кінцевого пункту А в кінцевий пункт не потрібно. У

цьому випадку кінцевий пункт А періодично передаватиме в кінцевий пункт повідомлення HEARTBEAT , щоб переконатися в працездатності кінцевого пункту В. Фрагмент HEARTBEAT містить спеціальну інформацію відправника. Отримувач фрагмента HEARTBEAT повинен відповісти фрагментом HEARTBEAT ACK , який містить інформацію, скопійовану з прийнятого фрагмента HEARTBEAT .

Фрагмент ABORT передається кінцевим пунктом, щоб різко припинити з'єднання. Цей фрагмент може містити інформацію про причину припинення з'єднання і може бути передано в одному пакеті з іншими керуючими фрагментами SCTR Однак у таких випадках він має бути останнім фрагментом у пакеті Якщо він передається не останнім у пакеті, то наступні фрагменти ігноруються. Фрагменти DATA не повинні входити до складу пакету, що містить фрагмент ABOPT .

Фрагмент SHUTDOWN використовується для плавного припинення з'єднання. Якщо програма верхнього рівня або керуюча програма хоче закрити з'єднання, то кінцевий пункт припиняє передачу нових даних на далекий кінець. Він буде чекати, поки не отримає підтвердження всіх переданих даних, а потім передасть на дальній кінець фрагмент SHUTDOWN , щоб закрити з'єднання. SHUTDOWN буде вказувати останній фрагмент - DATA , прийнятий від далекого кінця. Якщо це необхідно, віконний пункт може повторно передати дані користувача на далекий кінець і лише потім передати фрагмент SHUTDOWN .

Після прийому фрагмента SHUTDOWN кінцевий пункт може переконатися, що всі дані користувача, які він передав, підтверджені, і, якщо необхідно повторно передати дані на далекий кінець. Якщо справді все, що кінцевий пункт передавав раніше, отримано, він має передати фрагмент SHUTDOWN ACK .

Після отримання SHUTDOWN ACK відправник SHUTDOWN повинен - відповісти фрагментом SHUTDOWN COMPLETE і може стерти всю інформацію про з'єднання. Коли дальній кінець приймає фрагмент SHUTDOWN COMPLETE , він також може стерти всю інформацію з'єднанні. У цей момент з'єднання зруйноване.

Фрагмент ERROR передається для повідомлення про виявлені кінцевим пунктом помилкові ситуації. До складу фрагмента зазвичай входить повідомлення про причину помилки, щоб забезпечити можливість її подальшої обробки. Наприклад, кінцевий пункт міг отримати фрагмент неіснуючого потоку або фрагмент, де відсутні деякі обов'язкові параметри. Отримання фрагмента ERROR саме не вказує на непоправне стан. Переданий фрагмент ERROR просто може дати можливість приймачеві виправити помилковий стан. Якщо ясно, що помилковий стан непоправний, фрагмент ERROR може бути переданий у тій же дейтаграмі, що і фрагмент ABORT

Фрагмент COOKIE ECHO використовується тільки під час ініціювання - з'єднання. Коли кінцевий пункт отримує фрагмент 1MTi відповідає фрагментом INITACK , він включає до складу INITACK параметр cookie . Цей параметр містить особливу для кінцевого пункту та для його надання з'єднанню інформацію, тимчасову мітку та значення часу життя параметра cookie (рекомендується 5 секунд). Коли на далекий кінець приходить INITACK , копія cookie вводиться у фрагмент COOKIE ECHO , який передається у зворотному напрямку. COOKIE ECHO може передаватися в пакеті, який містить також фрагменти DATA . Однак у такому разі фрагмент COOKIE ECHO має бути першим фрагментом у пакеті.

Фрагмент COOKIE ACK передається у відповідь на фрагмент COOKIE ECHO . Тому COOKIE ACK використовується лише під час встановлення - з'єднання. Оскільки вміст фрагмента COOKIE ACK таке саме, яке було передано в INIT ACK , відправник INIT ACK може переконатися, що ініціатор з'єднання прийняв інформацію cookie правильно. Якщо фрагмент COOKIE ECHO був прийнятий без помилок і протягом вказаного для cookie часу життя, приймач COOKIE ECHO передає фрагмент COOKIE ACK . В іншому випадку передається фрагмент ERROR . Фрагмент COOKIE ACK може передаватися в тій же дейтаграмі, що і фрагменти DATA , але повинен бути першим фрагментом у цій дейтаграмі.

3.3.5. Фрагмент корисного навантаження DATA

Фрагмент *DATA* використовується для перенесення до і від UPL інформації користувача. Він має формат, показаний на рис. 3. 4 .



Рис. 3.4 Формат фрагмента DATA

Є можливість, що протоколу SCTP доведеться розділити повідомлення на сегменти. Таке може статися, якщо MTU тракту менше розміру повідомлення, яке потрібно надіслати. Через можливу сегментацію у формат фрагмента введено біти *Початок (B)* та *Кінець (E)*. Біт B показує, що фрагмент містить частину

першого сегмента повідомлення користувача, а біт E - фрагмент містить частину останнього сегмента повідомлення. Якщо повідомлення повністю вміщається в один фрагмент, обидва біти, B і E мають значення 0. Якщо повідомлення містить більше 2 сегментів, перший фрагмент першого сегмента повинен мати біт, рівний 1, а біт E -рівний 0, в той час як останній фрагмент останнього сегмента повинен мати біт, рівний 0, а біт E рівний - 1. Фрагменти всіх сегментів у проміжку між першим і останнім повинні мати обидва біти, E і B, рівними 1.

Біт U показує, що фрагмент належить невпорядкованому потоку даних. Іншими словами, порядок повідомлень користувача в потоці не відіграє ролі, і порядковий номер у потоці слід ігнорувати. У такому разі SCTP пропускає дані у верхній рівень без аналізу порядку надходження повідомлень. Однак SCTP все-таки повинен гарантувати, що сегментовані зі спілкування пройшли відновлювальну збірку до відправлення даних у верхній рівень.

Порядковий номер передачі (TSN) являє собою 32-бітове ціле число, яке ідентифікує фрагмент у контексті з'єднання. Цей номер не залежить від порядкового номера фрагмента в потоці і призначається SCTP , а не користувачем SCTP . Коли пункт передає фрагмент INIT , до його складу входить TSN , відповідний першому фрагменту DATA , який цей пункт планує передати. Таким чином, перший переданий фрагмент DATA завжди містить той же TSN , що і фрагмент INlT . Після цього TSN збільшується для кожного нового фрагмента DATA , що передається кінцевим пунктом цього з'єднання.

Ідентифікатор потоку (S) є 16-бітовим цілим числом, що визначає потік, якому належать дані. Порядковий номер у потоці (n) - це 16-бітове ціле число, що вказує положення повідомлення всередині потоку. Порядкові номери повідомлень у кожному потоці починаються з 0. Номер збільшується для кожного повідомлення, що передається в цьому потоці. Зауважимо, що сегментоване повідомлення повинне мати в кожному сегменті один і той самий порядковий номер у потоці.

Ідентифікатор протоколу корисного навантаження передається від користувача-відправника до SCTP на передавальному кінці і пропускається від SCTP до користувача-адресату на приймальному кінці. Він доступний користувачам для пропуску подальшої інформації про фрагмент, але SCTP не перевіряє цей ідентифікатор і не впливає на нього.

3.3.6 Встановлення з'єднання

Встановлення з'єднання зазвичай ініціює протокол верхнього рівня, який наказує SCTP встановити з'єднання. З'єднання може бути встановлено заздалегідь перед передачею трафіку даних. Наприклад, якщо мережевий адміністратор організує пучок з'єднувальних ліній ISUP в Softswitch і Softswitch використовує M 3 UA , дії, пов'язані з визначенням пучка з'єднувальних ліній, можуть змусити M 3 UA запросити в SCTP встановлення з'єднання. Подібним чином, з'єднання може бути встановлене, коли в обслуговування вводиться нова ланка ОКС 7 в SG , або коли вводиться в обслуговування новий діапазон CIC . Цей процес зображено на рис. 3.5.

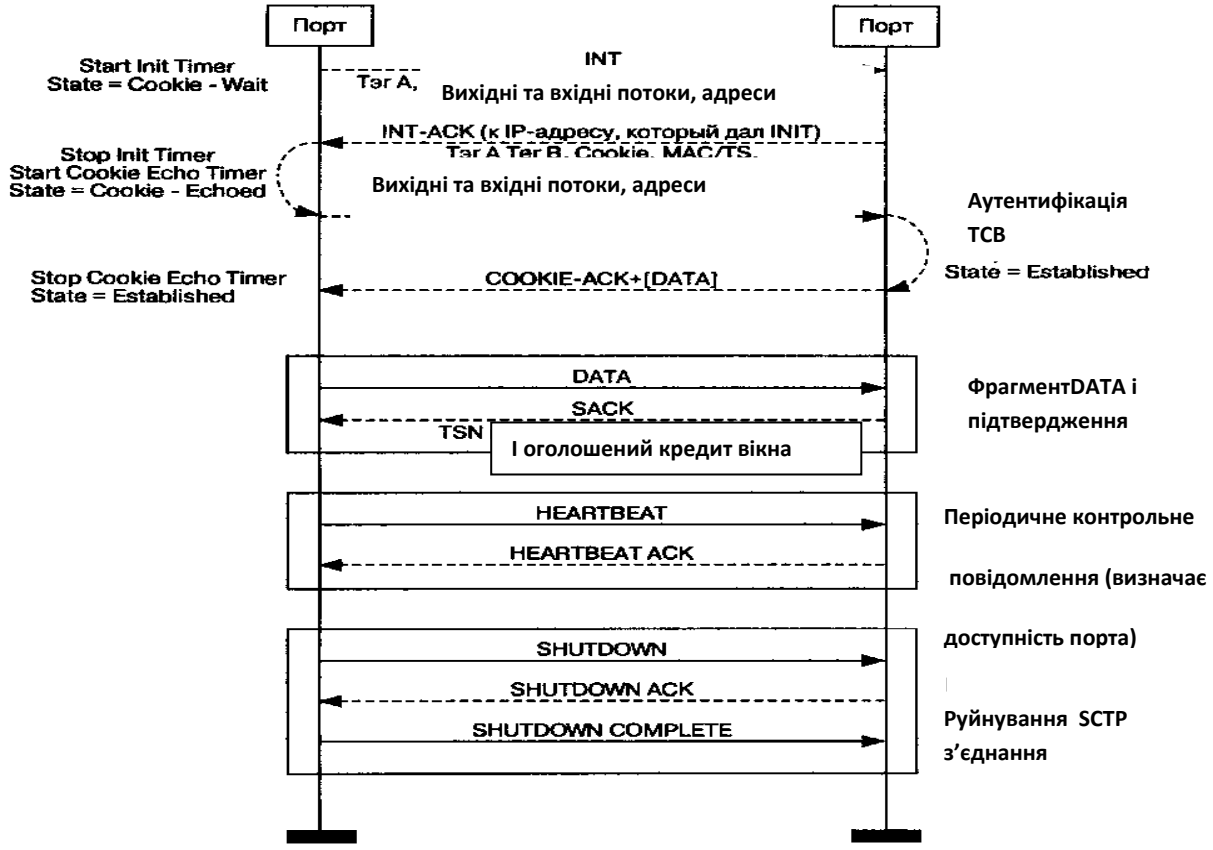


Рис. 3.5 Сценарій встановлення та руйнування SCTP - з'єднання

Він починається передачею на транспортну адресу віддаленого порту пакета SCTR, що містить фрагмент INIT , ініціюючи цим встановлення SCTP-з'єднання. Відправник запускає таймер і переходить у стан cookie - wait (очікування cookie).

Крім обов'язкових параметрів фрагмент INIT може містити також ряд додаткових параметрів та/або параметрів з довжиною, що варіюється. Наприклад, фрагмент INIT може містити одну або кілька адрес IPv4 і IPv6, або ім'я дозволеного хоста.

Віддалений порт, який приймає INIT , генерує фрагмент INIT - ACK і передає його на IP - адресу відправника INIT . INIT - ACK містить дані про cookie -станах, і, як тільки він приймається , відправник INIT зупиняє таймер і передає фрагмент COOKIE - ECHO . Запускається новий таймер, а відправник переходить у стан cookie - wait . Фрагмент INIT ACK також може містити низку адрес IPv4 і IPv6. Зважаючи на те, що фрагмент INIT ACK теж містить деяку кількість вхідних та вихідних потоків, обидва кінці з'єднання знають максимальну кількість потоків, які може передавати та приймати інша сторона. Кожен пункт повинен дотримуватися вимог іншого і не повинен передавати більше, ніж інший пункт може обробити. Після прийому фрагмента INIT ACK ініціатор з'єднання передає фрагмент COOKIE ECHO , вміст якого скопійовано з параметра cookie прийнятого фрагмента INIT ACK . Коли на дальній кінець з'єднання приходить COOKIE - WAIT і від нього надходить фрагмент COOKIE - ACK , обидва порти переходять у стан *з'єднання встановлено (established).*

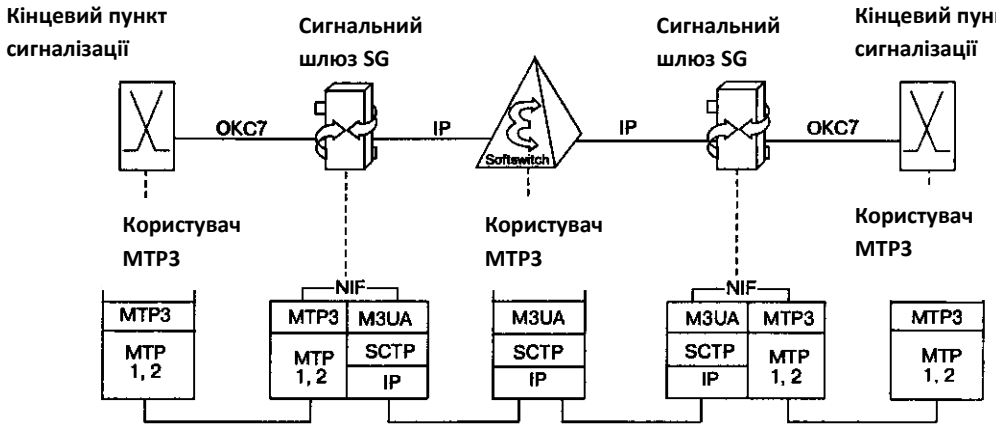
Надійне пересилання даних користувача досягається шляхом використання двох фрагментів. Перший - це фрагмент DATA , а другий - фрагмент SACK . Прийом фрагментів OATA підтверджується фрагментами ЗАСК, які також вказують на пропуски в послідовності передачі даних потоку. Періодично відбувається обмін фрагментами HEARTBEAT для підтримки з'єднання між портами на маршрутах, що діють, між транспортними адресами. Пара повідомлень HEARTBEAT / HEARTBEAT - ACK корисна і визначення часу подвійного пробігу (затримки підтвердження прийому) RTT між портами, що, своєю чергою, використовується обчислення розмірів вікон передачі. Численні невдалі спроби передати на порт фрагмент певного типу (або неодноразові - спрацьовування таймера при очікуванні SACK у відповідь на DATA) можуть означати, що поточна транспортна адреса недоступна.

SCTP- з'єднання можуть руйнуватися негайно (за допомогою повідомлення ABORT) або поступово (за допомогою сигнальної процедури SHUTDOWN / SHUTDOWN - ACK / SHUTDOWN COMPLETE), як показано у представленому сценарії. Зауважимо, що, на відміну від протоколу TCP , протокол SCTP не підтримує «напіввідкритий» стан, при якому одна сторона може продовжувати передачу даних, тоді як інша сторона вже закрита.

4 ХАРАКТЕРИСТИКА ПРОТОКОЛІВ АДАПТАЦІЙНИХ РІВНІВ SIGTRAN

4. 1 Функції протоколу M 3 UA

Раніше зазначалося, що завдання M 3 UA - забезпечити надання додатків у мережі I P послуг, аналогічних тим, які MTP 3 надає додаткам на кшталт ISUP в мережі ПРО КС 7. Пояс їм це на рис. 4.1, де показаний Softswitch , якому необхідно запустити програму типу ISUP . Взагалі кажучи, Softswitch може зробити це кількома способами. Наприклад, він може запустити ISUP поверх MTP 3 поверх M 2 UA (або M 2 PA) поверх SCTP , як це обговорюється у двох наступних параграфах. Або ж Softswitch може реалізувати ISUP поверх M 3 UA поверх SCTP , як показано на рис. 4.1. Різниця між цими двома способами визначається тим, де реально розташована функція MTP 3. У сценарії, показаному на рис. 4.1, звичайний протокол MTP 3 присутній у шлюзах SG, а MSUA просто забезпечує додатком ISUP в Softswitch віддалений доступ до функції MTP 3 в SG без відчуття додатком ISUP того , що функція MTP 3 не є локальною.



NIF = вузлова функція взаємодії

Рис. 4.1. Функції M 3 UA у Softswitch

Softswltch на рис. 7.8 може мати код пункту сигналізації, відмінний від коду, який має SG . У цьому випадку SG працює подібно до STP і сприймається зовнішньою мережею OKC 7 як STP . Зовнішня мережа 0 KC 7 розглядає Softswitch як звичайний пункт сигналізації OKC 7, доступ до якого досягається через один або кілька пунктів SG STR .

4.2 **Термінологія протоколу**

Перш ніж ми перейдемо до більш детального розгляду M 3 UA , необхідно обумовити деякі терміни, які застосовуються також до інших адаптаційних рівнів. Насамперед, під черкнем різночитання між терміном *сервер додатків AS { Application Server),* використаним раніше в контексті Vo - IP і Softswitch , і тим же терміном у розумінні робочої групи Sigtran для протоколів адаптаційного рівня. В останньому випадку під *сервером додатків AS* розуміється логічний об'єкт, який обробляє сигналізацію у певній галузі. Наприклад, AS може бути логічним об'єктом в Softswitch , який обробляє сигналізацію ISUP для конкретного діапазону ОКС 7 DCP / OPC / CIC . У рівній мірі, AS може бути логічним об'єктом у додатку бази даних, що обробляє сигналізацію.

Процес сервера додатків ASP (Application Server Process) є екземпляр AS , що нагадує концепцію процесів у мові специфікацій та описів SDL , що обговорюється в [4]. Сервер AS містить набір *процесів сервера програм.* Фактично, AS можна як список процесів ASP , частина яких активна, а частина перебуває у резерві. ASP може бути, наприклад, процесом в Softswitch , який в цей час обробляє сигналізацію ISUP . У стійкій мережі повинен бути принаймні один активний ASP і, принаймні, один резервний ASP для кожної програми. Один ASP може обслуговувати кілька серверів AS . Наприклад, Softswitch може мати кілька серверів AS , кожен з яких відповідає унікальній комбінації OPC / DPC . Цей самий Softswitch може мати лише один ASP , що обробляє всю сигналізацію ISUP (або два процеси AEP для резервування або для поділу навантаження).

Ключ маршрутизації (Routing Key) являє собою набір таких параметрів ОКС 7, як SLS , DPC , OPC або діапазон CIC , які визначають сигналізацію для деякого AS . Наприклад, якщо якийсь AS повинен обробляти сигналізацію ISUP для - певної комбінації OPC / DPC /діапазон CIC , то ця комбінація і є ключем маршрутизації для такого AS . У межах SG кожен ключ маршрутизації зазвичай вказує на один певний AS . Інакше кажучи, між ключами маршрутизації та AS зазвичай існує однозначна відповідність.

Відображення мережі (Network Appearance) - це таке її уявлення , яке дозволяє відокремити частину сигнального трафіку, потрібну для зв'язку між SG і ASP , від усього трафіку, що використовує те саме з'єднання SCTR . Уявімо, наприклад, міжнародний SG . Цей SG матиме принаймні один національний та міжнародний код пункту сигналізації. SG використовує національний варіант MTP для зв'язку в національній мережі та варіант ITU - T MTP – для зв'язку в міжнародній мережі, а тому він повинен бачити та розрізняти відповідні сигнальні потоки. Для зв'язку між SG і Softswitch повідомлення, що передаються і приймаються повинні поміщатися в контексті правильного відображення мережі, щоб можна було оперувати відповідною групою ліній на не-1P стороні SG .

4.3 Код пункту сигналізації

Кожен ASP необхідно асоціювати з кодом пункту сигналізації. Однак, призначення кодів пунктів для процесів ASP є абсолютно гнучким. Наприклад, всі ASP , приєднані до певного SG можуть спільно використовувати той же код пункту, що і цей SG . У такому разі комбінація SG та процесів ASP видно мережі ОКС 7 як єдиний кінцевий пункт сигналізації. Або ж всі ASP , приєднані до одного SG можуть мати один і той же код пункту, який відрізняється від коду пункту сигналізації, присвоєного цьому SG . У такому разі SG буде видно мережі 0 КС 7 як STP , а об'єднані загальним кодом ASP - як єдиний пункт сигналізації, розташований за цим STP .

Ще одним варіантом призначення кодів може бути присвоєння кожному ASP свого коду пункту або групам ASP - різних загальних кодів, відмінних від коду, присвоєного SG . У цьому випадку SG видно як STP , а кожен ASP (або група процесів ASP) - як один кінцевий пункт сигналізації. Справа в тому, що якщо якийсь ASP або група ASP може зв'язуватися з мережею 0 КС 7 не через один, а через два SG , то цей ASP або ця група ASP повинні мати код пункту, який відрізняється від кодів цих двох SG . У такому сценарії шлюзи SG працюють як транзитні пункти сигналізації STR .

4.4 Примітиви

Щоб надавати послуги верхньому рівню прозоро (так, щоб програма не відчувала факт використання функцій MTP 3, вбудованих у SG замість функцій локальної MTP), МОЗ U A повинен надавати верхньому рівню ті ж самі примітиви, які надає MTP 3. Це такі примітиви:

- *MTP - Transfer request* передається з верхнього рівня M 3 UA , щоб запросити перенесення повідомлення в певний пункт на значення.
- *MTP - Transfer indication* використовується M 3 UA , щоб пропустити вхідне повідомлення у верхній рівень.
- *MTP - Pause indication* передається M 3 UA у верхній рівень, щоб вказати, що передача сигналів у певний пункт призначення має бути припинена. Цей примітив використовується, наприклад, коли пункт призначення недосяжний.
- *MTP - Resume indication* передається M 3 UA у верхній рівень, щоб вказати, що можна відновити передачу сигналів до пункту призначення.
- *MTP – Status indication* передається M 3 UA у верхній рівень, щоб інформувати цей рівень про деякі зміни, що виникли в мережі ОКС 7, таких як перевантаження або недоступність під системи-користувача в пункті призначення.

Розглянемо приклад програми ISUP в Softswitch , якому потрібно передати повідомлення до мережі ОКС 7. Додаток передає запит MTP - Transfer request в M 3 UA , а M 3 UA передає його в SCTP як фрагмент DATA , який необхідно передати по певному з'єднанню SCTP і в певному потоці. SCTP забезпечує надходження фрагмента DATA в SG , де вміст цього фрагмента - проходить в M 3 UA , який передає його до функції взаємодії в SG . Функція взаємодії пропускає його в MTP 3 на стороні мережі ОКС 7 шлюзу SG , який перебирає коректну маршрутизацію повідомлення далі в мережу ОКС 7.

У протилежному напрямі процес відбувається аналогічно. Повідомлення надходить у SG і проходить від MTP 3 до функції взаємодії , а від функції

взаємодії надходить у M 3 UA . На основі параметрів DPC / OPC /діапазон CIC повідомлення ОКС 7 вибираються відповідний AS і відповідний ASP . Якщо активні більше одного ASP , то вибирається один з них (відповідно до алгоритму поділу навантаження). M 3 UA формує повідомлення передачі SCTP як фрагмента DATA по відповідному з'єднанню SCTP і у відповідному потоці. У пункті призначення фрагмент DATA проходить у M 3 UA , який пропускає інформацію цього фрагмента в додаток, використовуючи примітив MTP - Transfer indication .

4.5 Повідомлення протоколу M 3 UA

До складу M 3 UA входить ряд повідомлень між однорівневими об'єктами M 3 UA , загальний формат яких показано на рис. 4.2. Формат містить заголовок та вміст повідомлення. Заголовок є загальним всім рівнів адаптації. Для рівня M 3 UA версія протоколу дорівнює 0000 0001. Клас повідомлення може бути наступним:

- **00** Повідомлення управління;
- **01** Повідомлення пересилання;
- **02** Повідомлення *експлуатаційного управління мережею сигналізації ОКС7* (SSNM);
- **03** Повідомлення експлуатаційного управління станом ASP (ASPSM);
- **04** Повідомлення експлуатаційного керування трафіком ASP (ASPTM);
- **05** Резерв для класу повідомлень, що стосуються IUA та що забезпечують транспортування прикордонних примі- **BOBQ** .921/ Q 931;
- **06** Резерв для класу повідомлень адаптації користувача, що відносяться до M 2 UA ;
- **07** Резерв для класу повідомлень без встановлення з'єднання ня, що відносяться до SUA ;

- **08** Резерв для класу повідомлень, орієнтованих на спів-
  єднання і відносяться до SUA ;
- **09** Повідомлення експлуатаційного управління ключем марш-
  рутизації (RKM);
- **10** Резерв для класу повідомлень експлуатаційного управління
  лення ідентифікатором інтерфейсу M2UA;
- **11** Резерв для класу повідомлень M2PA;
- від **12** до **127** резервовано комітетом IETR
- від **128** до **255** резервовані для визначених IETF
  розширення класу повідомлень.

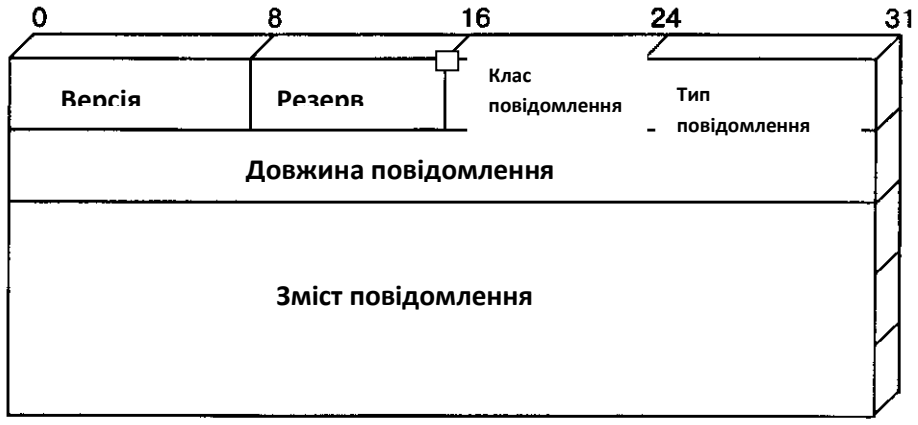


Рис. 4.2 Загальний формат повідомлення M 3 UA

Коли M 3 UA пересилає інформацію користувача між SG та Softswrtch , як було описано раніше, він виконує це шляхом передачі повідомлень M 3 UA DATA . Ці повідомлення формуються як фрагменти SCTP DATA . При передачі повідомлення DATA поле класу повідомлення має значення 1, тип повідомлення має значення 1, як це показано в табл. 4.

Окрім упаковки повідомлень користувача у формат повідомлень M 3 UA DATA , M 3 UA передбачає інші повідомлення між однорівневими MO3 U A - об'єктами, так що ці об'єкти можуть обмінюватися інформацією, що відноситься до мережі ПРО КС 7 в цілому. Наприклад , якщо пункт призначення стає недоступним, то SG повідомляється про це за допомогою повідомлень експлуатаційного керування мережею сигналізації ОКС 7.

Додаток ISUP у Softswitch також повинен повідомлятися про цю подію, щоб вона не намагалася передавати повідомлення, які не можуть досягти свого пункту на значення. M 3 UA в Softswitch може попереджати про таку подію за допомогою примітиву MTP - Pause indication . Але M 3 UA - не MTP 3 і повідомлення експлуатаційного управління мережею сигналізації не проходять прямо від SG до SG . Тому M 3 UA в Softswitch дізнається, що пункт призначення недоступний, за допомогою іншого повідомлення M 3 UA крім повідомлення DATA . У табл. 4 наводиться список типів повідомлень M 3 UA .

Таблиця 4.1

Повідомлення M 3 UA

Ім'я повідомлення	Клас повідомлення	Код класу повідомлення	Код типу повідомлення
Error (ERR)	MGMT	00	00
Notify (NTFY)_____	MGMT	00	01
Data _____	Transfer	01	01
Destination Unavailable (DUNA)	SSNM	02	01
Destination Available {DAVA)	SSNM	02	02
Destination StateAudit(DAUA)	SSNM	02	03
SS7 NetworkCongestion State(SCON)	SSNM	02	04

Продовження таблиці 4.1

Destination User Part Unavailable (DUPU)	SSNM	02	05
Destination Restricted (DRST)	SSNM	02	06
ASP Up (ASPUP)_____	ASPSM	03	01
ASP Down (ASPDN) _____	ASPSM	03	02
Heartbeat (BEAT)_____	ASPSM	03	03

ASP Up Acknowledgment (ASPUP ACK)	ASPSM	03	04
ASP Down Acknowledgment (ASPDN ACK)	ASPSM	03	05
Heartbeat Acknowledgment (BEAT ACK)	ASPSM	03	06
ASPActive(ASPAC)_____	ASPTM	04	01
ASP Inactive {ASPIA) _____	ASPTM	04	02
ASP Active Acknowledgment (ASPAC ACK)	ASPTM	04	01
ASP Inactive Acknowledgment (ASPIA ACK)	ASPTM	04	02
Registration Request (REG REQ) _____	RKM	09	01
Registration Response (REG RSP) _____	RKM	09	02
Deregistration Request (DEREG REQ)_____	RKM	09	03
Deregistration Response (DEREG RSP)	RKM	09	04

До *повідомлень експлуатаційного управління (Management Messages)* відноситься повідомлення *ERR -помилка (Error)* про те, що прийнято непередбачене повідомлення або повідомлення з невірним вмістом, а також повідомлення *NTFY -повідомлення (Notify)* для передачі інформації про певні події, що відносяться до М 3 UA . Наприклад, повідомлення NTFY можна використовувати, щоб інформувати про зміну стану ASP . До складу повідомлень *експлуатаційного керування мережею сигналізації (Signaling Network Management Messages)* М 3 UA входять: повідомлення *DUNA* - адресат недоступний (Destination Unavailable), що передається з SG у всі зацікавлені процеси ASR щоб повідомити їх про недоступність пункту призначення в мережі ОКС 7, повідомлення *DAVA* - ад ресат доступний (Destination Available), яке в ASP перетворюється на примітив MTP - Resume indication , повідомлення *DAUD* - перевірка стану пункту призначення (Destination State Audit), повідомлення *SCON* про перевантаження мережі

ОКС 7 (SS 7 Network Congestion), повідомлення *DUPU - підсистема* - користувач у пункті призначення недоступна (Destination User Part Unavailable), яке в ASP відображається в примітиві MTP - Status indication і повідомлення DRST -доступ до пункту призначення обмежений (Destination Restricted).

До складу повідомлень M 3 UA входять такі *повідомлення експлуатаційного управління станом ASP (ASP State Management Messages): ASPUP* - ASP включений (ASP Up) та *ASPUP ACK* - підтвердження - включення ASP (ASP Up Acknowledgment), *ASPDN - ASP* вимкнений (ASP Down) та ASPDN ACK - підтвердження вимкнення ASP (ASP Down Acknowledgment), *BEAT* та *BEATACK* - повідомлення про працездатність (Heartbeat messages), а також *повідомлення екс плуатаційного управління трафіком AEP (ASP Traffic Management Messages),* за допомогою яких організується передача трафіку між SG та одним або декількома ASP (розподіл навантаження), а також *повідомлення експлуатаційного управління ключами маршрутизації (Routing Key Management Messages).*

4.6 Протокол M2 U A

Використання M2 UA ілюструє рис. 4.3. У цьому сценарії два сигнальних шлюзу SG забезпечують інтерфейс із зовнішньою мережею ПРО КС 7. Обидва шлюзи приєднані до Softswitch . На стороні Softswitch шлюзів SG ми маємо M 2 UA поверх SCTP поверх IP , а на стороні ОКС 7 - стандартну MTP стека ОКС 7. У Softswitch ми маємо стандартний протокол MTP 3, який працює поверх M 2 UA та IR У звичайній мережі ОКС 7 MTP 3 використовує послуги протоколу MTP 2. Однак у зображеному на рис. 4.3 сценарії MTP 3 у Softswitch використовує послуги MTP 2, який розташований у SG , не усвідомлюючи того, що той не є локальним. Функція M 2 UA - забезпечити - прозорий доступ зі стандартного MTP 3, що знаходиться в Softswitch до стандартного MTP 2, що знаходиться в SG .

Пояснимо це докладніше. Раніше була описана ситуація, в якій Softswitch підтримує функції ISUP , але не реалізує функції нижніх рівнів стека ОКС 7. Зокрема, MTP 3 в самому Softswitch не реалізований, що призводить до того, що Softswitch «не бачить» мережу ОКС 7, як це може робити будь-який логічний об'єкт, що безпосередньо реалізує MTP 3. У тому числі, він не передає і не приймає повідомлення експлуатаційного управління мережею сигналізації. Якщо ж бажано, щоб Softswitch був залучений в експлуатаційне керування мережею сигналізації, то однією з можливостей є реалізація MTP 3 в Softswitch і використання M 2 UA по верх SCTP для доступу до функцій MTP 2 в SG . Це дозволило б Softswitch краще «бачити» мережу ОКС 7, а також тісніше взаємодіяти зі шлюзом сигналізації SG . Фактично SG стає в такому випадку віддаленим терміналом сигналізації, що становить , з точки зору мережі ОКС 7, логічний елемент Softswitch .

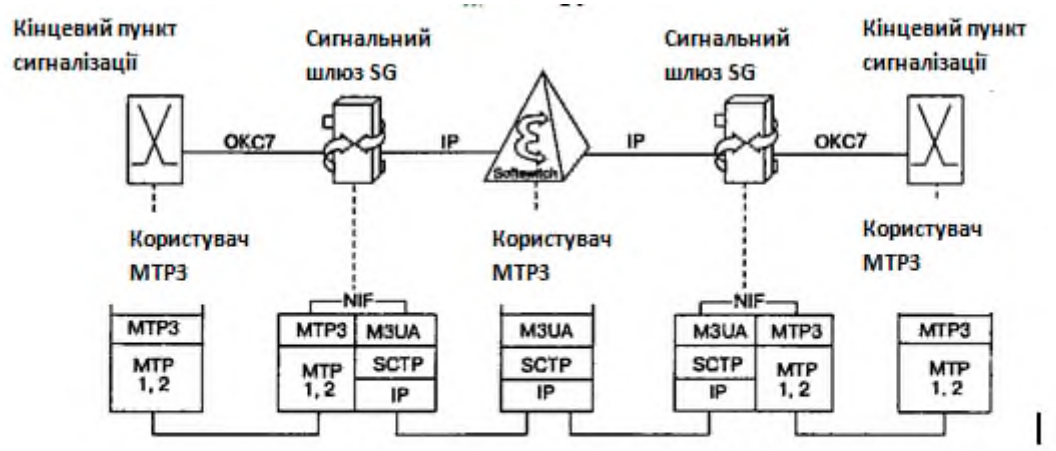


Рис. 4.3 Функції M 3 UA у Softswitch

У прикладі на рис. 4.3. Додаток MTP 3 в Softswitch може приймати такі сигнальні повідомлення експлуатаційного управління мережею, як *TransferAllowed { TFA)* та *TransferProhibited (TFP).* Протокол MTP 3 може використовувати цю інформацію при визначенні того, як маршрутизувати повідомлення такого користувача MTP 3 верхнього рівня, як ISUP .

M 2 UA використовує концепції, аналогічні обговорюваним у попередньому параграфі для M 3 UA . До них входять поняття AS і ASP . Він передбачає також аналогічні повідомлення, такі як ASPUP , ASPDN , ASPAC , ASPIA , NTFY , BEAT , ERR , та відповідні підтвердження. Ці повідомлення використовуються так само, як вони використовуються в M 3 UA , з тією різницею, що протоколи ASP в M 2 UA виконують інші функції. У M 3 UA протокол ASP може мати відношення до характеристик, подібних до DPC / OPC / діапазон CIC , або іншого набору характеристик; а M 2 UA протокол ASP є окремим випадком MTP 3 в такому вузлі, як Softswitch .

Повідомлення, що передаються між однораноговими об'єктами M 2 UA мають той же формат, що і повідомлення M 3 UA (див. рис. 4.2); відрізняється тільки поле Message Type загального заголовку. Для M 2 UA ці повідомлення мають інші коди класу - коди 6 та 10, а повідомлення експлуатаційного управління станом ASP та трафіком ASP є спільними для всіх рівнів адаптації. Всі ці міркування виправдовують рішення заощадити місце на описі повідомлень M 2 UA , функції яких цілком очевидно випливають з вищевикладеного.

4.7 Протокол M2PA

Розглянемо рисунок 4.4, який ілюструє сферу застосування M 2 PA .

Ідея M 2 PA - у прозорому з боку протоколу MTP 3 і вищележачих протоколів транзиті сигнальних одиниць через IP , тобто для MTP 3 протокол M 2 PA не відрізняється від традиційного MTP 2. Незмінними залишаються всі функції мережевого рівня ОКС 7: балансування навантаження між ланками одного пучка за допомогою поля селектора сигнальної ланки (SLS), виявлення несправностей, процедури перемикання на альтернативний маршрут (change - over) і повернення на початковий (change - back), контроль перевантаження ланки за допомогою порогів, що задаються, і т. д. M 2 PA має реєстраційний номер порту 356
Незважаючи на деяку подібність M2UA і M2PA , між ними є принципові відмінності. Хоча протокол M 2 UA і дозволяє Softswitch використовувати

стандартний MTP 2 у віддаленому сигнальному шлюзі SG , але M 2 PA суворо відповідає версії MTP 2. І показане на рис. 4.4 з'єднання SG - Softswitch фактично є ланкою ОКС 7, тоді як аналогічне з'єднання на рис. 4.3 таким не є.

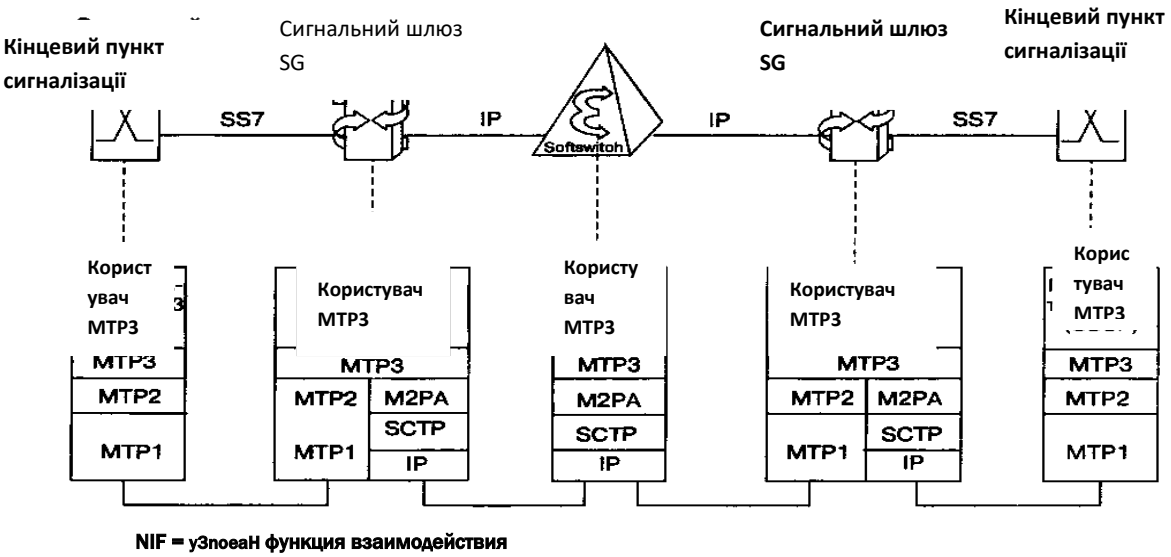


Рис.4.4 Функції M 2 PA в Softswltch

Прямим наслідком цієї різниці є те, що SG , який використовує M 2 UA фактично служить для показаного на рис. 4.3. Softswitch віддаленим терміналом сигналізації. У той же час SG , який використовує M 2 PA , вже сам по собі є вузлом сигналізації ; у нього є власний код пункту сигналізації, і він фактично є STP на базі IP . Це означає, що SG може виконувати такі функції сигналізації верхнього рівня, як SCCP . Наприклад, SG , що використовує M 2 PA , може виконувати перетворення глобальної адреси - Global Title Translation (GTT), - а сигнальний шлюз SG на базі M 2 UA такі функції виконувати не може.

Вибір між M 2 UA та M 2 PA цілком надається проектувальнику або Оператору мережі. Все залежить від функцій, які мають виконуватися у певних вузлах мережі. Якщо, наприклад, SG повинен виконувати такі функції, як GTT , то відповідним вибором буде M 2 PA . З іншого боку, якщо SG призначений просто як термінал сигналізації ОКС 7 для вузла lP -мережі (такого як Softswitch), то достатньо буде M 2 UA .

Тепер кілька слів про реалізацію цих функцій у M 2 PA . Існують три типи сигнальних одиниць ОКС 7 на рівні MTP 2: значущі сигнальні одиниці MSU , які

переносять корисне навантаження користувача; одиниці LSSU , які переносять інформацію про стан сигнальної ланки, і заповнюють сигнальні одиниці FISU , які передаються, коли іншої інформації для передачі немає. Протокол M 2 PA підтримує повідомлення аналогічних типів IP -мережі, крім FISU . Відсутність у M 2 PA еквівалента FISU пояснюється принципами функціонування IP -мережі, що стосується коректної роботи трактів сигналізації в IP -мережі, то для цього використовується вищезгадане повідомлення SCTP BEAT , а повідомлення M 2 PA для пересилання даних включають функції підтвердження. Т.ч., M 2 PA є два повідомлення: повідомлення User Data та повідомлення Link Status .

Повідомлення User Data в M 2 PA є просто сигнальною одиницею MSU , з якої виключено кілька стандартних полів ОКС 7, і містить індикатор довжини LI (Length Indicator), акт службової інформації SIO (Service Information Octet) і поле сигнальної інформації SIF (Signaling Information Field). Поля Flag, Backward Sequence Number (BSN), Backward Indicator Bit (BIB),

Forward Sequence Number (FSN), Forward Indicator Bit (FIB) та Check Bits у склад User Data не входять . LI включено до складу User Data тільки тому, що деякі національні варіанти ОКС 7 використовують два резервні біти Ll як покажчик пріоритету.

Повідомлення Link Status обмінюються однорангові об'єкти M 2 PA щоб інформувати один одного про поточний стан тракту . Link Status аналогічно LSSU в ОКС 7 і також містить поле status (стан), яке може приймати такі значення:

- Alignment (фазування);
- Proving Normal(Підтвердження нормального стану);
- Proving Emergency (підтвердження аварійного стану);
- Ready (готовність);
- Processor Outage (пошкодження процесора);
- Processor Outage Ended (відновлення процесора);
- Busy (зайнятий);
- Busy Ended (звільнився);

- Out of Service (виведений із обслуговування);
- In Service (введений в обслуговування).

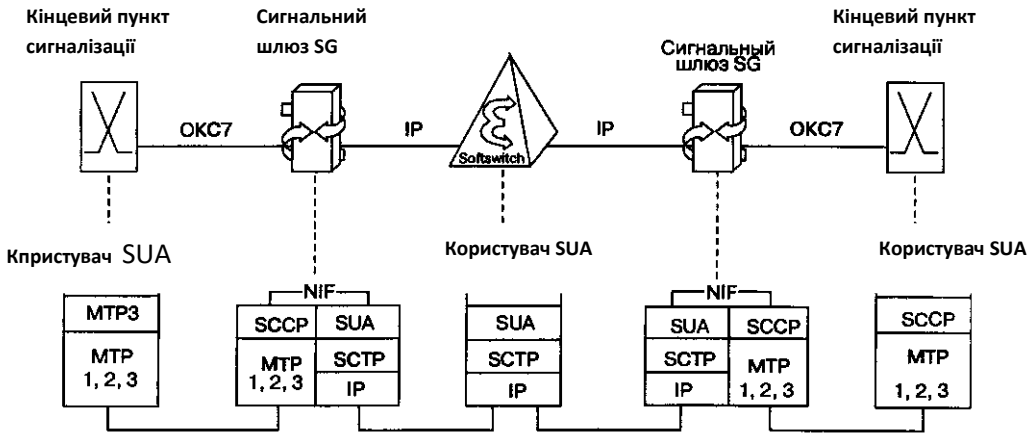
4.8 Протокол SU A

SUA - протокол транспортування інформації SCCP через мережу IP { Transporting SCCP over iP) визначено робочою групою Sigtran для транспортування по мережі IP з використанням SCTP сигнальних - повідомлень підсистеми SCCP стека ОКС 7 (несуть, насамперед, інформацію TCAP і RANAP). По суті, SUA дублює послуги SCCP шляхом підтримки надійного пересилання повідомлень користувача SCCP , включаючи підтримку послуг без з'єднання (клас 0 і 1), так і орієнтованих на з'єднання (клас 2 і 3). SUA підтримує також послуги експлуатаційного управління SCCP , призначені для керування станом віддалених пунктів призначення та підсистем SCCP . Крім того, в деяких конфігураціях SUA виконує ще й функції перетворення пеки пекла і маршрутизації.

Таким чином, протокол SUA забезпечує взаємодію з мережею ОКС 7 на вищому рівні, ніж це робить M 3 UA (і тим більше M 2 UA , M 2 PA). У сигнальному шлюзі завершують роботу (термінуються) протоколи MTP і SCCP , а до ASP передається лише корисний вміст повідомлень SCCR Протокол SUA має за реєстрований IANA номер порту 14001. Він має також зареєстрований IANA ідентифікатор протоколу корисного навантаження SCTR .

Для транспортування повідомлень без з'єднання SCCP та SUA сполучаються в шлюзі SG . Саме там (з точки зору пункту сигналізації ОКС 7) розташований користувач SCCP . Повідомлення ОКС 7 маршрутизуються до SG на основі коду пункту сигналізації та номера підсистеми SCCP , а потім шлюз сигналізації маршрутизує повідомлення SCCP до віддаленого кінцевого пункту IP . Якщо існують резервні кінцеві пункти IP , шлюз сигналізації може поділити навантаження між активними кінцевими пунктами IP , використовуючи циклічний

метод.



NIF = вузлова функція взаємодії

Рис.4.5 Функції SUA у Softswitch

Зауважимо, що при розподілі навантаження, створюваного повідомленнями TCAP , вибір кінцевого пункту пересилки відбувається тільки для першого повідомлення в діалозі TCAP . Наступні повідомлення в тому ж діалозі TCAP завжди передаються в кінцевий пункт, який обраний для першого повідомлення, доки не буде отримана інформація про стан кінцевих пунктів, і сигнальний шлюз не буде поінформований про стратегію розподілу повідомлень кінцевих пунктів IP .

Формат загального заголовка повідомлення та TLV , раніше визначений - для M 3 UA , однаково застосовується і для SUA .

Повідомлення без з'єднання використовуються для трафіку класу 0 та класу 1 протоколу.

Існують два повідомлення без з'єднання: CLDT і CLDR :

- Повідомлення Connectionless Data Transfer відповідає повідомленням unitdata (UDT) , extended unitdata (XUDT) і long unitdata (LUDT) у SCCP . Воно використовується для пересилання даних між однорангові ЗіА для трафіку класу 0 і класу 1.

- Повідомлення Connectionless Data Response відповідає повідомленням послуги unitdata (UDTS), послуги extended unitdata (XUDTS) та послуги long unitdata (LUDTS) в SCCP . Воно передається як відповідь у CLDT , щоб інформувати про помилки у повідомленні CLDT , якщо використовується відповідна опція.

Повідомлення, орієнтовані на з'єднання, використовуються для трафіку протоколу класу 2 та класу 3:

- Connection Request (CORE) використовується, щоб запросити сигнальне - з'єднання між двома кінцевими пунктами. Це повідомлення відповідає Connection Request (CR) у SCCP.
- Connection Acknowledgement (COAK) використовується для позитивної - відповіді на Connection Request . Це повідомлення відповідає повідомленню Connection Confirm (CC) у SCCR
- Connection Refusal (COREF) використовується для негативної відповіді на запит Connection Request . Це повідомлення відповідає повідомленню Connection Refusal (CREF) у SCCP.
- Connection - oriented Data Transfer (CODT) використовується для передачі даних по сигнальному з'єднанню. Воно відповідає повідомленням Data Form 1 (DT 1), Data Form 2 (DT 2), та Expedited Data (ED) у SCCP .
- Connection - oriented Data Acknowledgement (CODA) використовується одноранговим кінцевим пунктом для підтвердження отримання даних. Це повідомлення використовується лише для повідомлень протоколу класу 3. Воно відповідає повідомленню Data Acknowledgement (AK) у SCCP.
- Release Request (RELRE) використовується для запиту зруйнувати сигнальне з'єднання. Це повідомлення відповідає Connection Released (RLSD) у SCCP.
- Release Complete (RELCO) використовується для підтвердження руйнування сигнального з'єднання. Усі ресурси, відведені з'єднанню, мають бути звільнені. Це повідомлення відповідає повідомленню Release Complete (RLC) в SCCR

- Reset Request (RESRE) використовується для запиту почати заново присвоєння порядкових номерів повідомленням у пункті- відправнику та пункті-одержувачі, які асоційовані з сигнальним з'єднанням. Це повідомлення відповідає повідомленню Reset Request (RSR) у SCCR
- Connection - oriented Error (COERR) використовується для вказівки, що в протокольному блоці даних була помилка. Це спілкування відповідає повідомленню Protocol Data Unit Error { ERR) у SCCR
- Connection-oriented Inactivity Test {COIT) відповідає повідомлення - lnactivityTest (IT) в SCCR

SUA підтримує ті ж *повідомлення MGMT ,* що і M 3 UA , але також надає інформацію про стан підсистеми SCCP . Повідомлення DUNA , DAVA , DRST , SCON та DAUD можуть опціонально містити номер підсистеми SubSystem Номер (SSN). Крім того, повідомлення DUNA , DAVA , DRST і SCON можуть опціонально утримувати параметр SubSystem Multiplicity Indicator (SMI).

SUA підтримує ті ж *повідомлення RKM ,* що і M 3 UA , але пара метр Routing Key відрізняється тим, що він містить опції для адрес джерела і пункту призначення та для діапазонів адрес.

На закінчення зазначимо, що, з одного боку, за рахунок термінування в сигнальному шлюзі «зайвого» протоколу досягається більш ефективне використання смуги пропускання IP -мережі, але, з іншого боку, з цієї причини втрачається можливість передачі через SUA інформації протоколу ISUP , оскільки адресації SUA використовує рівень MTP 3 ОКС 7.

Сигнальний шлюз може виконувати *перетворення глобальних адрес GTT (Global ТШе Translation)* для визначення пункту призначення повідомлення SCCP . Сигнальний шлюз маршрутизує повідомлення no глобальною адресою, яка є такими цифрами, що є у вхідному повідомленні, як номер викликаної сторони або ідентифікаційний номер мобільного абонента. Для транспортування повідомлень, орієнтованих на з'єднання, SCCP та EiA

сполучаються в сигнальному шлюзі, щоб об'єднати дві ділянки з'єднання, необхідні при орієнтованій на з'єднання пересилання даних між кінцевим пунктом сигналізації ОКС 7 і кінцевим пунктом IP . Маршрутизація повідомлень здійснюється сигнальним шлюзом до сигнальних пунктів там ОКС 7 на основі коду пункту призначення (у полі адреси MTP 3) і до кінцевих пунктів IP на основі IP -адреси (в заголовку SCTP).

4.9 Протокол IUA

У ISDN сигнальну інформацію користувача, наприклад, зі спілкування Q .931, переносить ланковий рівень Q .921. Еквівалентною специфікацією Sigtran в мережі IP є IUA . Кадри Q .921 можуть пропускатися з ISDN в мережу IP з ідентичними реалізаціями Q .931 у кожній мережі, причому жодна з них не розпізнає жодних відмінностей у транспортуванні, що лежить в основі. Протокол IUA певний у документі RFC 3057 підтримки протоколів Q .931 і QSIG , причому, ця підтримка поширюється як у доступ ISDN на первинної швидкості (PRA), і на базовий доступ ISDN (BRA). Запропоновано також розширення IUA для DPNSS / DASS 2. Реєстраційний - номер порту для IUA дорівнює 9000.

4.10 Протокол V 5 UA

Універсальний інтерфейс мережі доступу V 5.2 підтримує підключення до місцевої АТС аналогових телефонних ліній, доступ ISDN на базовій швидкості, доступ ISDN на первинній швидкості та абонентський доступ інших типів, як це описано в [5] і, більш детально, в [11]. Т.к. в процесі конвергенції мережею зв'язку та переходу до NGN місцеві АТС замінюються керованими Softswitch медіа-шлюзами, то між системою доступу та Softswitch знадобиться SG , як показано на рис. 4.6. Протокол V 5 UA дає можливість додаткам V .2 в Softswitch

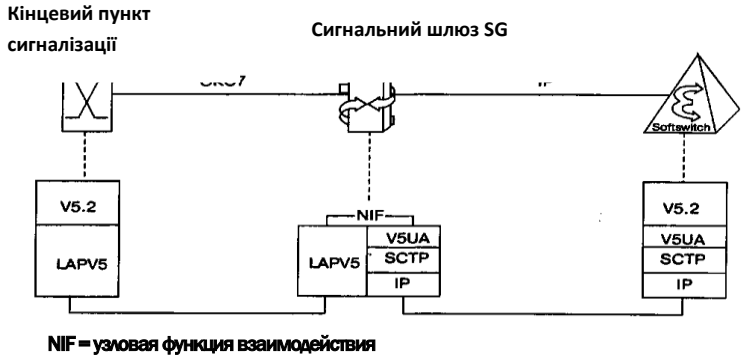


Рис. 4.6. Протокол V 5 UA

використовувати в шлюзі SG на стороні мережі доступу власні функції V 5.2. Протокол V 5 UA має реєстраційний номер порту 5675.

4.11 Приклади мережевих конфігурацій

Вихід за межі можливостей традиційних мереж зв'язку, зумовлений характером сьогоднішнього мультимедійного трафіку та потребами в мультисервісному його обслуговуванні, призвів до якісного перетворення всієї мережевої структури, і з'явилася концепція мережі наступного покоління *NGN (Next Generation Network),* суть побудови якої зводиться до конвергенції мереж різних технологій, під керуванням Softswitch .

З позицій мереж передачі даних NGN - це мережа Інтернет наступного покоління. З позицій мереж мобільного зв'язку цього покоління навіть надано номер 3G . З позицій традиційної телефонії NGN сьогодні сприймається як мережа пакетної комутації під управлінням Softswitch , що підтримує широкосмуговий абонентський доступ та мультисервісне обслуговування трафіку.

Загальними характеристиками NGN , визначеними ITU та ETSI є поділ функцій перенесення інформації та функцій управління перенесенням інформації через мережу, а також відокремлення функцій послуг та додатків від власне зв'язкових функцій. Таким чином, йдеться про розподілену архітектуру, в якій зв'язок між компонентами здійснюється виключно через відкриті інтерфейси. Але ми в цьому розділі почнемо розмову про NGN з обговорення прикладів мережевих конфігурацій з Softswitch , запропонованих консорціумом IPCC .

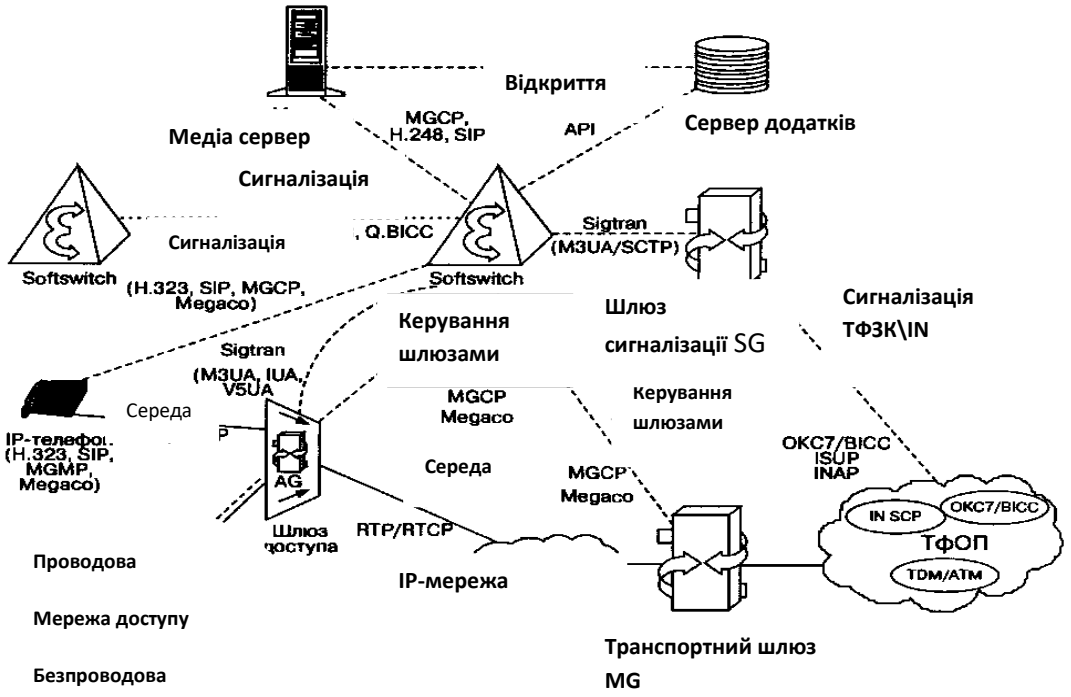


Рис. 4.7 Приклад архітектури NGN

Першим таким прикладом є мережева конфігурація, представлена на рис. 4.7. Елементами зображеної цьому малюнку мережі є Softswitch , сервер додатків *AS (Application Server),* шлюз між ТФОП та IP -мережею *TG (Trunk Gateway),* шлюз доступу *AG (Access Gateway),* шлюз сигналізації *SG (Signaling Gateway)* та транспортний (медіа) сервер *MS (Media Server).* Softswitch у цьому прикладі виконує функції MGC - F , R - F і A - F , розглянуті раніше, обробляє всю сигналізацію, керує TG , AG і відповідним виділенням медіа-ресурсів, проводить аутентифікацію викликів, а також забезпечує отримання облікової інформації. Крім того, кожен Softswitch взаємодіє з іншими Softswitch за протоколами SIP / SIP - T , H.323 або BICC .

Сервер програм *AS* реалізує логіку послуг. Виклик, який вимагає - додаткової послуги, або може бути переданий від Softswitch до AS для подальшого керування цією послугою, або сам Softswitch може отримувати від AS інформацію, необхідну для виконання логіки послуги. Сервер додатків AS може сам управляти MS або передати управління ним Softswitch

.

На транспортний шлюз TG надходять потоки користувальницької (мовленнєвої) інформації з боку ТФОП, він перетворює цю інформацію в пакети і передає її за протоколом IP в мережу з маршрутизацією пакетів, причому робить все це під управлінням Softswitch .

Шлюз доступу *AG* служить інтерфейсом між IP -мережею і проводовою або бездротовою мережею доступу, передає сигнальну інформацію до Softswitch , перетворює користувальницьку інформацію і передає її або до іншого порту цієї ж IP -мережі, або в іншу мережу з комутацією пакетів, або до TG для наступної передачі до мережі з комутацією каналів. Функціональним об'єктом MG - F у складі AG також управляє Softswitch . Сигнальний шлюз *SG* забезпечує доставку до Softswitch сигнальної інформації , що надходить з боку ТФОП, а також перенесення сигнальної інформації у зворотному напрямку.

Медіасервер *MS* може виконувати такі завдання, як, наприклад, передачу записаних оголошень та накопичення цифр номера, хоча в більшості випадків цифри накопичує шлюз Access Gateway . Сервером MS може керувати або Softswitch , або AS , або обидва ці мережні елементи. На рис. 4.8 показаний приклад мережі доступу з урахуванням протоколу V 5 і ISDN . Шлюз доступу AG обмінюється сигнальною інформацією V 5 і ISDN з мережею доступу і є

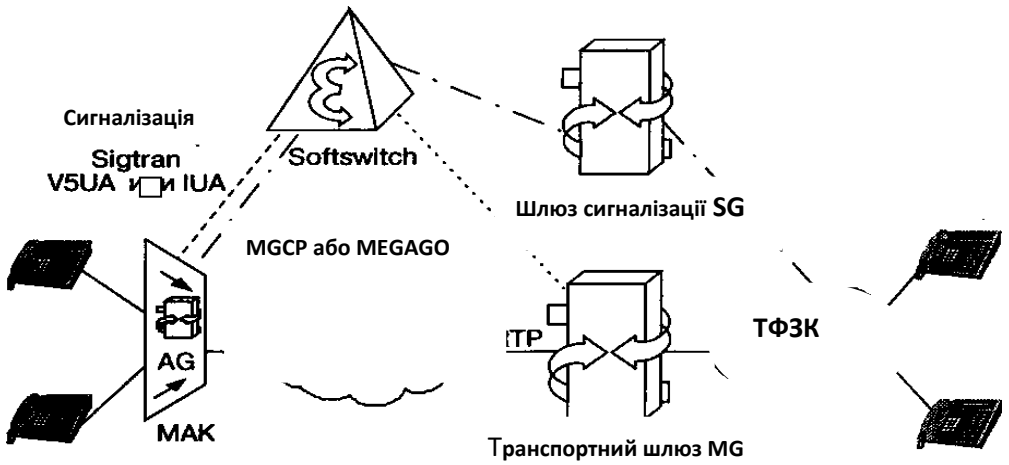


Рис. 4.8 Пример с ISDN и V5

закінченням фізичного з'єднання, по якому переноситься сигнальна інформація V 5 або ISDN , а потім передає цю інформацію по IP -мережі до Softswitch за допомогою протоколів сигналізації Sigtran (V 5 UA або IUA), розглянутих

раніше. Мовленнєву інформацію AG перетворює в пакетну форму, а потім передає її у вигляді пакетів протоколу RTP до портів цієї ж або іншої IP -мережі або до шлюзу TG , що перетворює пакетовану мову назад в TDM -форму і за тим, що передає її в мережу ТФЗК.

ВИСНОВКИ

У магістерській роботі розглянуто архітектуру, можливість та функціональні вимоги до протоколу . SIGTRAN для транспортування сигнальних повідомлень . У частині архітектури розглядаються взаємозв'язки між функціональними - та фізичними об'єктами, що використовуються для транспортування сигнальної інформації, включаючи конфігурацію керування транспортними шлюзами . Gateway) та інші сценарії, де може вимагатися транспортування сигнальної інформації.

У частині вимог описуються функціональні та якісні вимоги до транспортування сигнальної інформації, наприклад, управління потоком, послідовності доставки та інших функцій, які можуть бути потрібні для конкретних протоколів сигналізації мережі з комутацією каналів.

У роботі розглянуто основні положення щодо застосування протоколу передачі інформації управління потоком (Stream Control Transmission Protocol — SCTP), розробленого робочою групою IETF SIGTRAN для транспортування сигнальної інформації через інфраструктуру мережі IP . Наведено відомості щодо специфіки транспортування інформації сигналізації через мережу IP (адресація, маршрутизація). Розглянуто також використання адаптаційних рівнів, необхідних для транспортування сигналізації із застосуванням протоколу SIGTRAN .

ПЕРЕЛІК ПОСИЛАНЬ

1. Гольдштейн Б . С. , Пінчук О.В., Суховицький О.Л. IP-телефонія. - М: Радіо і зв'язок, 2001. - 336с.

2. Оліфер В.Г., Оліфер Н.А. Комп'ютерні мережі. Принципи, технології, протоколи. 2-ге видання. - СПб.: Пітер, 2005. - 864с.

3. Гольдштейн Б.С. Протоколи мережі доступу. Том 2. - М.: Радіо та зв'язок, 1999. 314с.

4. Ягофаров Т.М. VoIP виходить на новий виток розвитку. Комп'ютерний Огляд , 2002. №14.

5. Будніков В.Ю., Пономарьов Б.А. Технології забезпечення якості обслуговування мультисервісних мережах./Вісник зв'язку, 2000. №9

6. Осадчук О.В., Матвєєв С.М. Стандарт мультимедійного зв'язку H.323. /Мережі, 1999. №8, №9

7. http://cdo.bseu.by/library/ibs1/toppage2.htm

8. http :// www . protocols . ru / index . php

9. http :// www . osp . ru / nets /1999/08-09/24. htm

10. http :// www . voip 2 u . uk / Techno /

11. http :// cdo . bseu . by / library / ibs 1/ applic _ l / video / h 323/ h 323_ rus

12. http :// iptop . net / service / index . php

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ

Презентація

до магістерської кваліфікаційної роботи

на тему: « **Побудова мереж IP –телефонії на базі протоколу SIGTRAN**»

Виконав: студент групи ТСДМ-63 Стецюк В.Р.

Керівник: КТН, доцент Лаврінець К.Г.

Київ-2025

Об’єкт дослідження – сигналізація у мережі IP-телефонії.

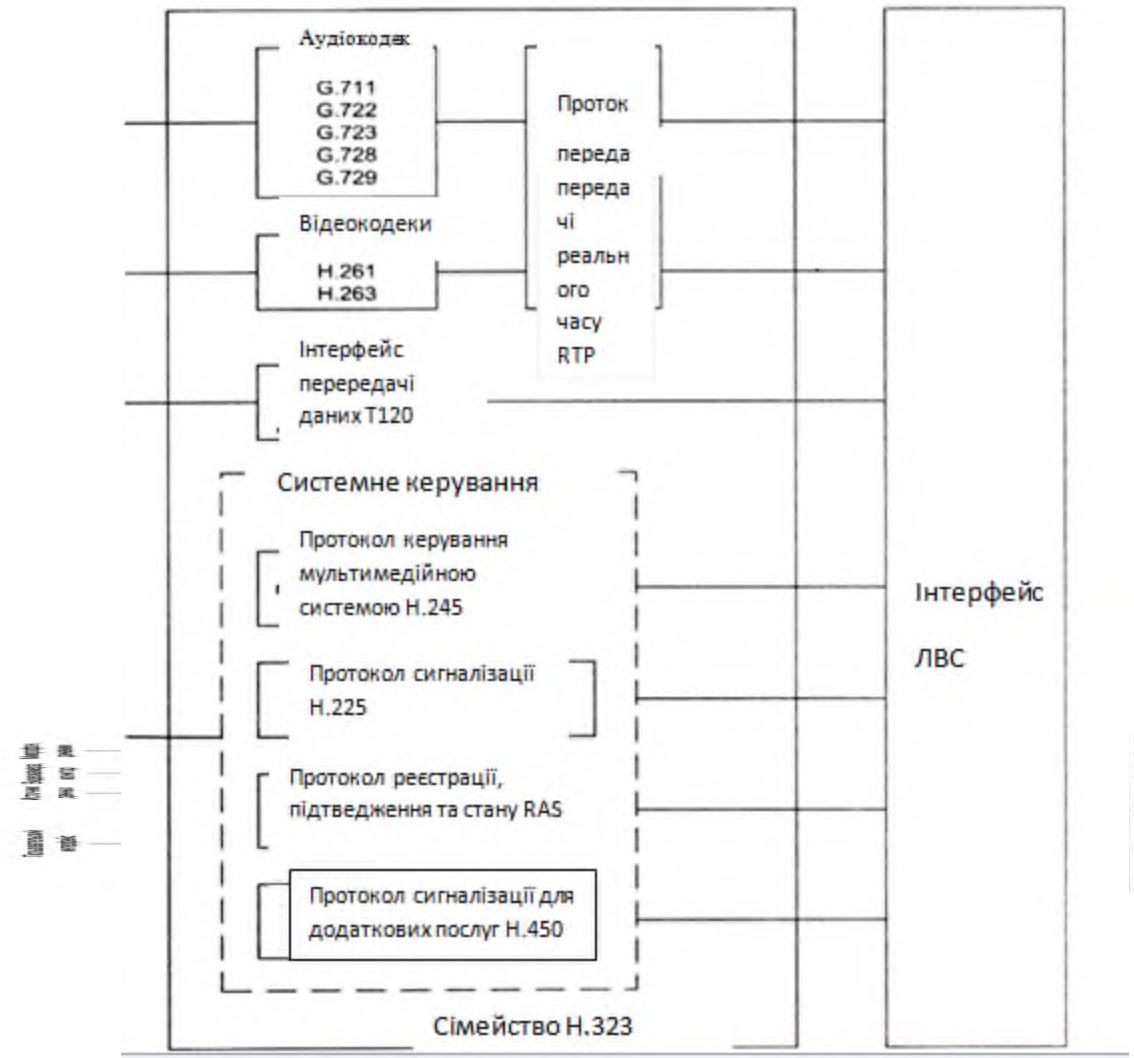
Предмет дослідження – дослідження принципів побудови мереж IP-телефонії з використанням протоколу SIGTRAN .

Мета роботи – розробити методику побудови мереж IP-телефонії з використанням протоколу SIGTRAN .

Методи дослідження – логічний аналіз та виявлення можливостей практичного використання мереж IP-телефоні на основі протоколуSIGTRAN .



Керування дзвінками в мережі IP-телефонії


Аудіокодек
G.711
G.722
G.723
G.728
G.729
Відеокодеки
H.261
H.263
Інтерфейс передачі даних T120
Проток
переда
переда
чі
реальн
ого
часу
RTP
Системне керування
Протокол керування мультимедійною системою H.245
Протокол сигналізації H.225
Протокол реєстрації, підтвердження та стану RAS
Протокол сигналізації для додаткових послуг H.450
Сімейство H.323
Інтерфейс
ЛВС

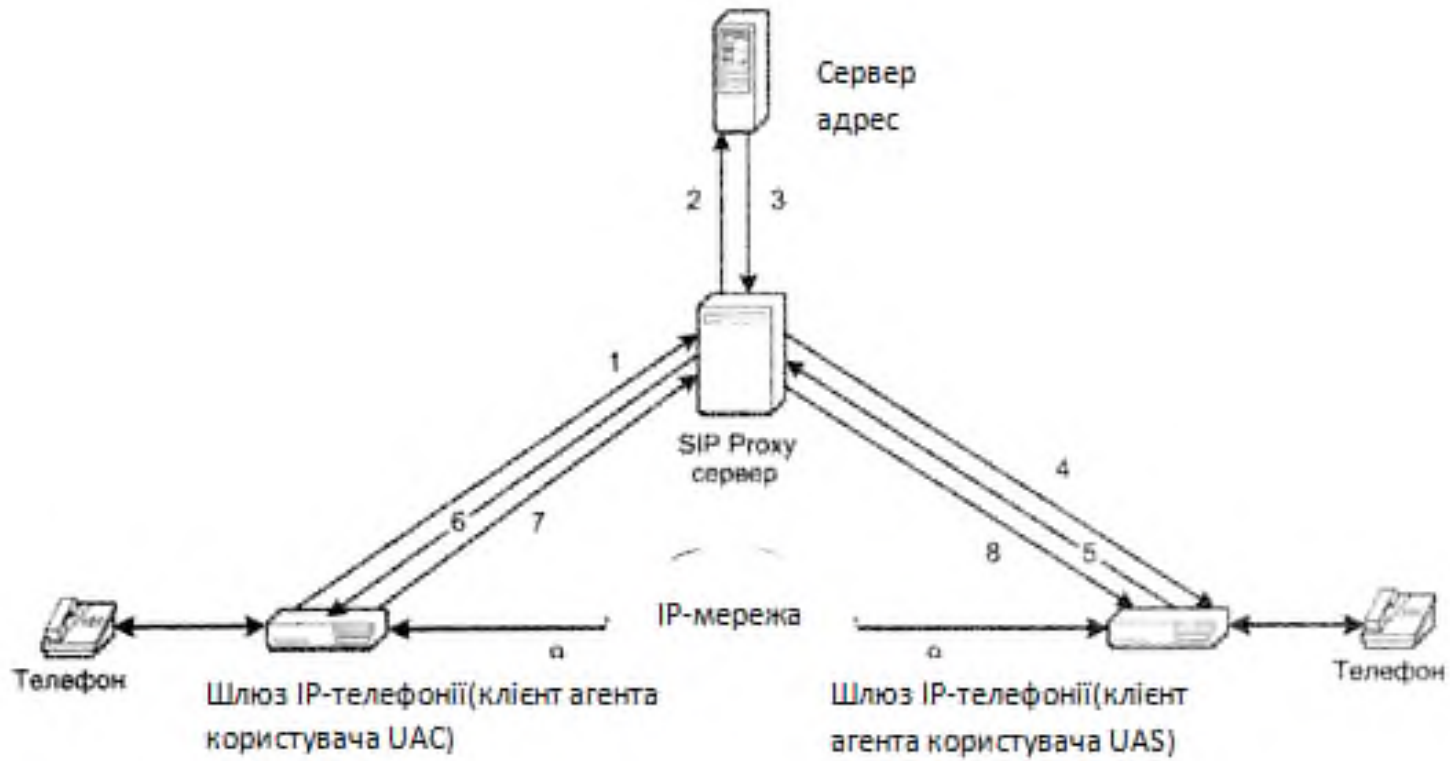
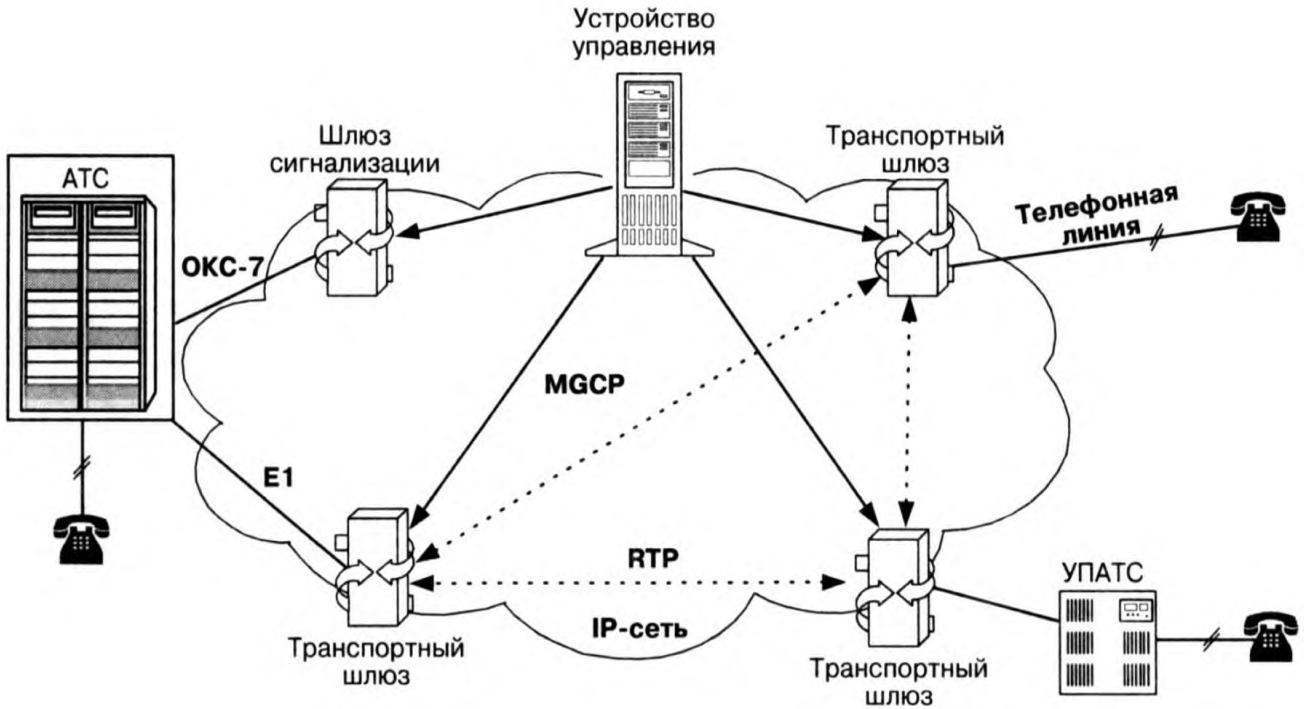
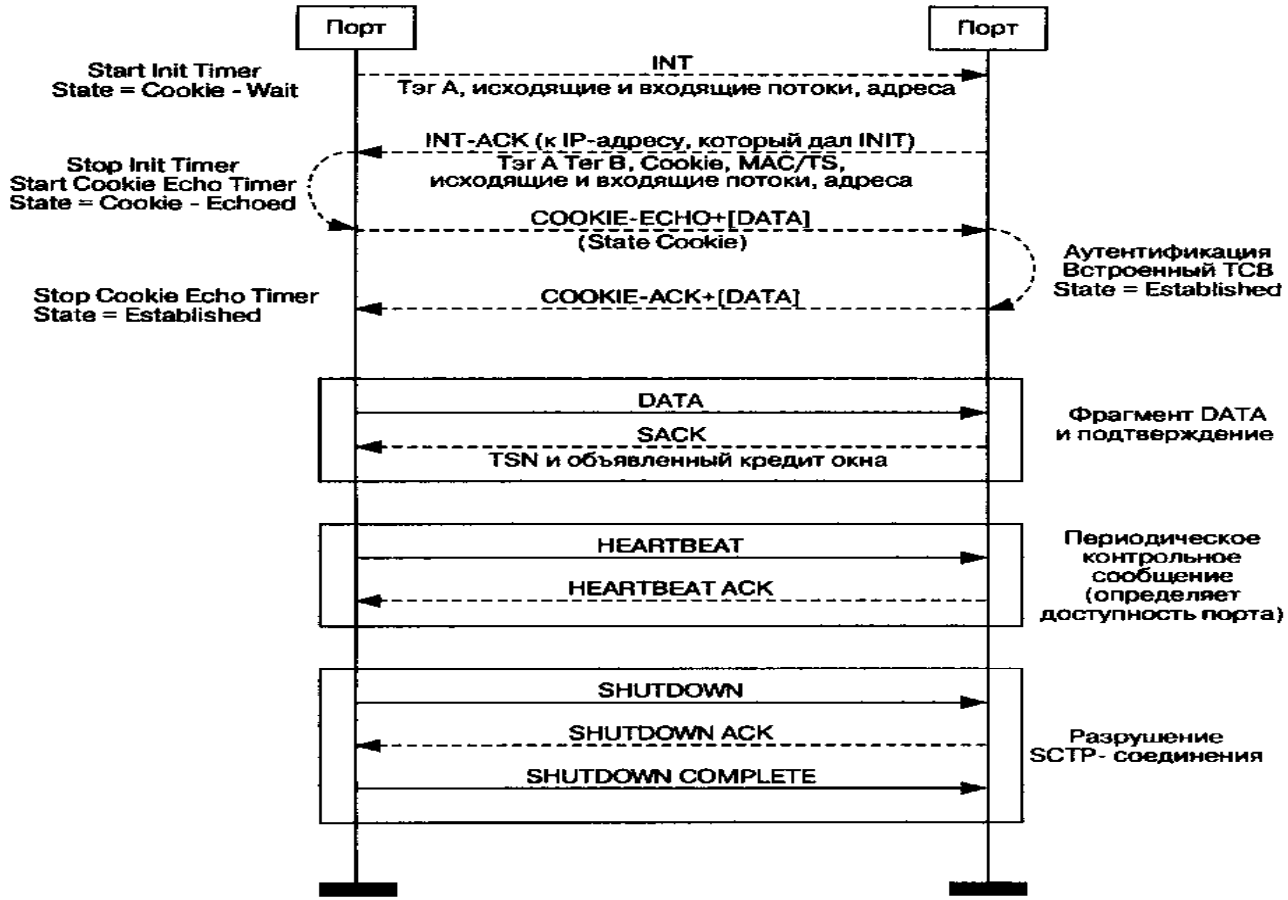


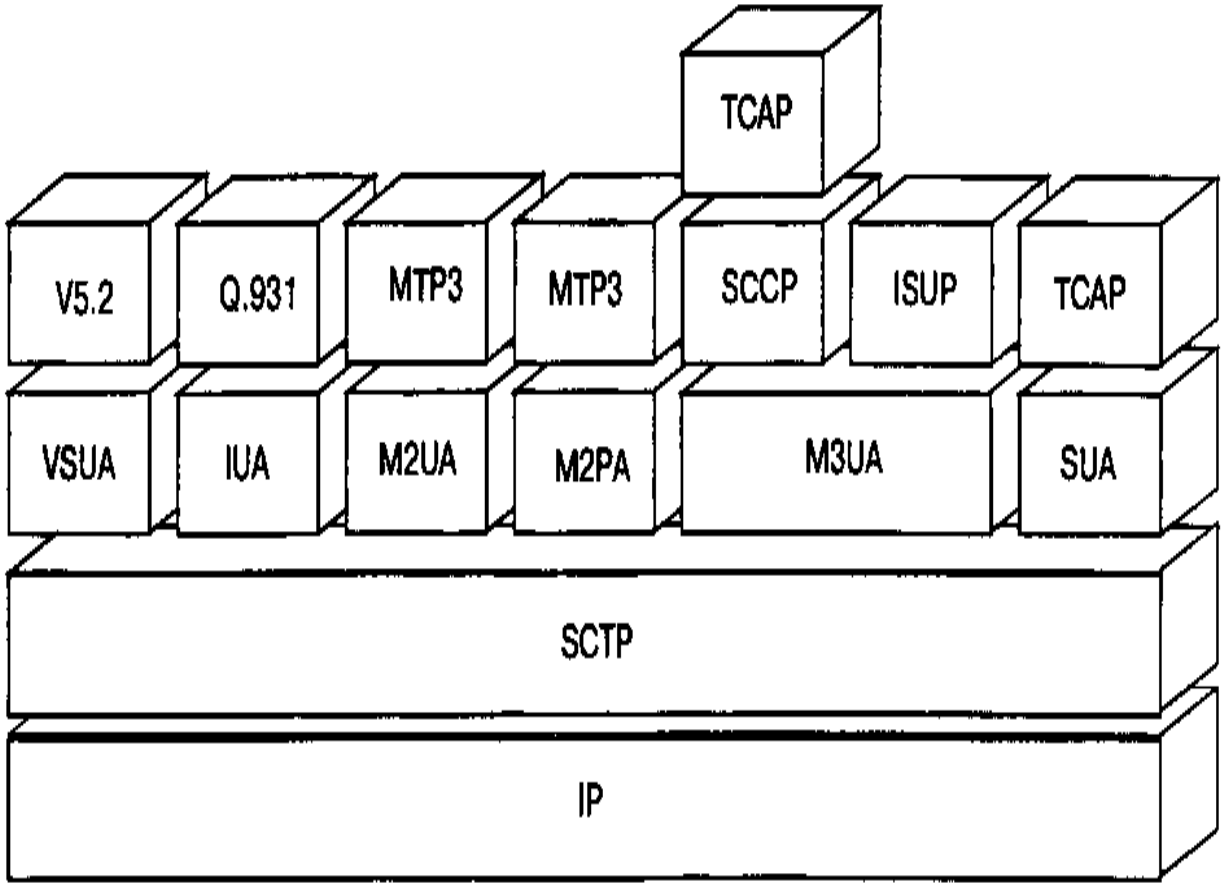
Схема сигналізації за протоколом SIP



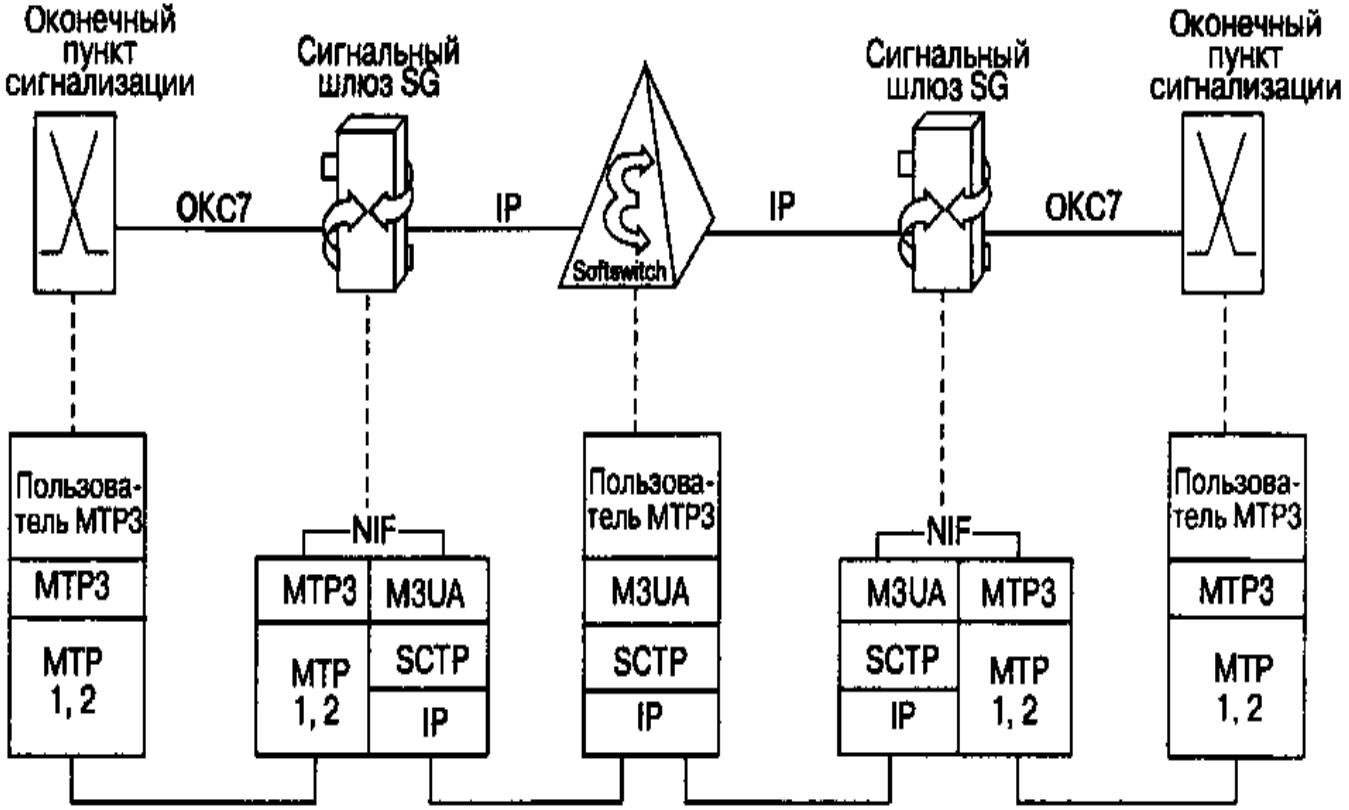
Архітектура мережі, що базується на протоколі MGCP



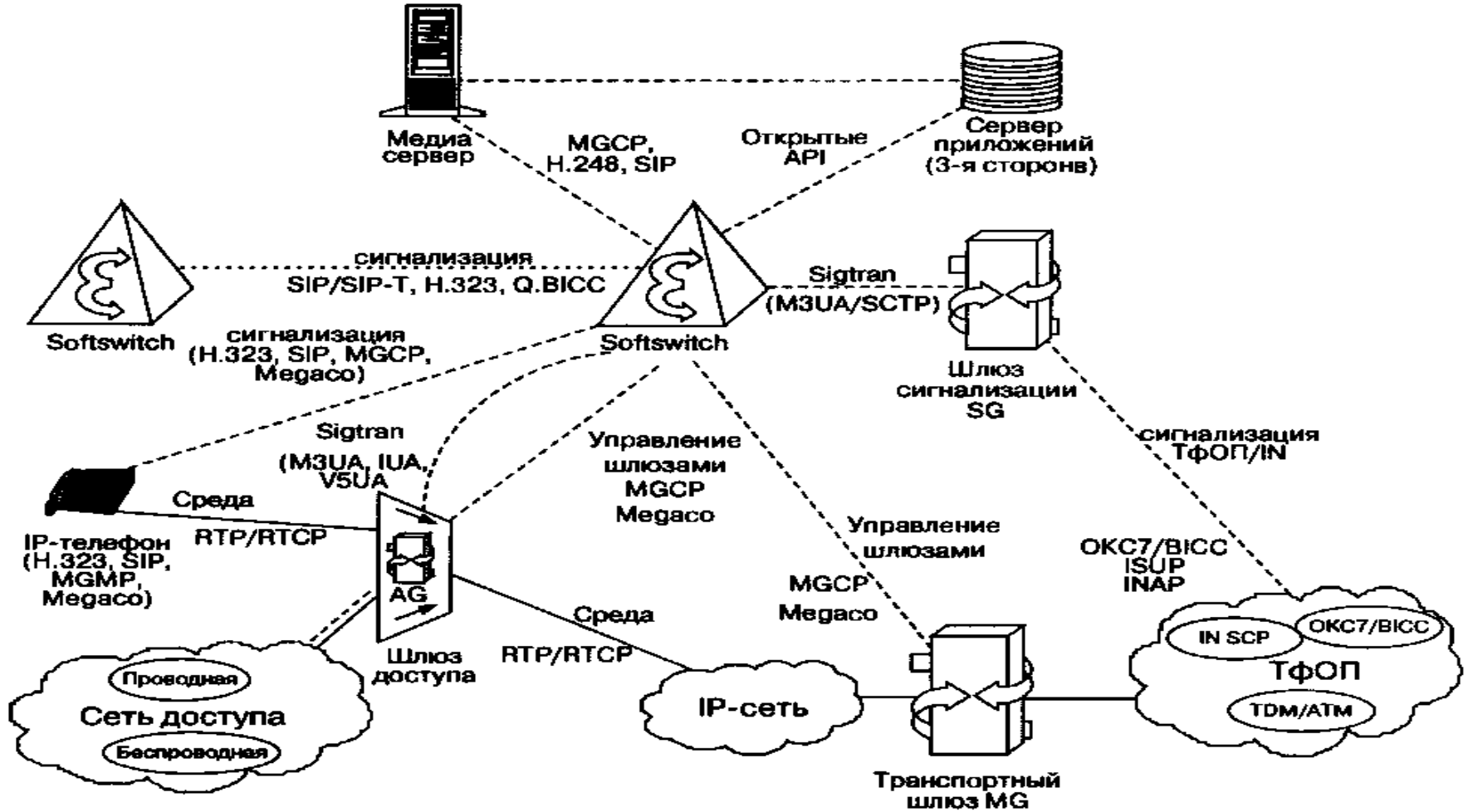
Встановлення та руйнування з'єднання з використанням протоколу MGCP



Архітектура протоколу Sigtran



Функції протоколу M 3 UA в Softswitch



Приклад архітектури мережі з використанням протоколу Sigtran

ВИСНОВКИ

У магістерській роботі розглянуто архітектуру, можливість та функціональні вимоги до протоколу . SIGTRAN для транспортування сигнальних повідомлень .

У частині архітектури розглядаються взаємозв'язки між функціональними та фізичними об'єктами, що використовуються для транспортування сигнальної інформації, включаючи конфігурацію керування транспортними шлюзами . Gateway) та інші сценарії, де може вимагатися транспортування сигнальної інформації.

У частині вимог описуються функціональні та якісні вимоги до транспортування сигнальної інформації, наприклад, у уравління потоком, послідовності доставки та інших функцій, які можуть бути потрібні для конкретних протоколів сигналізації мережі з комутацією каналів.

У роботі розглянуто основні положення щодо застосування протоколу передачі інформації управління потоком (Stream Control Transmission Protocol — SCTP), розробленого робочою групою IETF SIGTRAN для транспортування сигнальної інформації через інфраструктуру мережі IP . Наведено відомості щодо специфіки транспортування інформації сигналізації через мережу IP (адресація, маршрутизація). Розглянуто також використання адаптаційних рівнів, необхідних для транспортування сигналізації із застосуванням протоколу SIGTRAN .