ЗМІСТ

ВСТУП

Що таке телефонія знає не тільки кожна доросла людина, але навіть будь-яка дитина. Істотно менша кількість людей може пояснити, що таке Інтернет. І вже зовсім небагато знають, що ховається під терміном Інтернет-телефонія. Хоча зрозуміло, що новий термін вийшов шляхом з'єднання двох старих: Інтернет і телефонія. Звідси слідує достатньо просте визначення Інтернет-телефонії - це технологія передачі телефонних мовних повідомлень по мережі Інтернет.

Робота пристроїв в мережі Інтернет здійснюється з використанням спеціального Інтернет-протоколу (Internet Protocol - IP). В даний час протокол IP використовується не тільки в мережі Інтернет, але і в інших мережах передачі даних з пакетною комутацією (локальних, корпоративних, регіональних і ін.). І у всіх цих мережах, у принципі, є можливість передавати

мовні повідомлення з використанням пакетів даних. Такий спосіб передачі мови і одержав назву IP-телефонія . За кордоном звичайно уживається абревіатура VoIP - Voice over IP, хоча часто використовують вужчий термін

Інтернет-телефонія.

Інтерес різних суб'єктів ринку телекомунікаційних послуг (операторів зв'язку, провайдерів Інтернет, виробників устаткування і користувачів) до даного виду зв'язку незвичайно зріс останніми роками у зв'язку з розробкою нових стандартів і протоколів, коли IP-телефонна розмова впритул наблизилася за якістю до телефонної розмови по класичних телефонних мережах. Цей інтерес пояснюється тим, що IP-телефонія дозволяє істотно економити необхідну смугу пропускання каналів, що неминуче веде до зниження тарифів, особливо на міжміські і міжнародні телефонні розмови. Проте не все так гладко на шляху впровадження нової технології: є проблеми із забезпеченням крізної якості телефонного зв'язку, утруднена спільна робота устаткування різних виробників, потрібен нове, достатньо дороге апаратне і програмне забезпечення і ін.

На сторінках вітчизняних і зарубіжних телекомунікаційних журналів останнім часом розвернулася дискусія з приводу визначення місця і ролі IP-телефонії в подальшому розвитку засобів передачі мови. Погляди сторін, що беруть участь в дискусії, різко протилежні.

Одні з них стверджують, що майбутнє належить тільки протоколу IP мається на увазі універсальність застосування даної технології для передачі будь-яких видів інформації (голосу, даних, відео) і заміну всіх інших мереж на мережу з пакетною комутацією на базі протоколу IP. Часто доводиться чути, що дні традиційної телефонії з комутацією каналів визнані і через 10-15 років від неї вже нічого не залишиться.

Прихильники протилежних поглядів указують на те, що не дивлячись на великі темпи зростання об'єму трафіку IP-телефонії за останні роки (150-200%), його частка в США складає близько одного відсотка від трафіку класичної телефонії, а у всьому світі і того менше. Навіть з урахуванням всіх оптимістичних прогнозів оператори мереж зв'язку і в перспективі одержуватимуть основний

прибуток від надання послуг телефонних мереж з комутацією каналів. Аргументами на користь цих доводів є існуючі проблеми із забезпеченням необхідної якості передачі мови по публічних каналах Інтернет, порівняно менша надійність існуючих IP-мереж, трудність управління такими мережами.

Схоже істина десь посередині. Дійсно, IP-телефонія - не панацея для вирішення всіх телекомунікаційних проблем. Але в той же час її використання дозволяє пропонувати користувачам абсолютно нові, неможливі для традиційної телефонії сервіси і додатки. Та і сам чинник економіїі витрат на телефонний зв'язок грає не останню роль навіть з урахуванням нижчого, але прийнятнішого, якості передачі розмови. Все це говорить про те, що технологія IP-телефонії вигідна всім: і користувачам, і операторам мереж, і виробникам устаткування.

У міжнародних організаціях і форумах йде безперервна розробка нових стандартів і протоколів, пов'язаних з передачею мови по мережах з пакетною комутацією. Виробники апаратного і програмного забезпечення регулярно представляють на ринок свої нові продукти. Одним з них є технологія заснована на використанні протоколу MGCP.

1.ЗАГАЛЬНІ ПРИНЦИПИ ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ

1.1. Мережа Інтернет і протокол IP

Про технологію і мережу Інтернет і використовуваному в ній протоколі IP (Internet Protocol) є величезна кількість інформації. Далі приведені лише основні положення, які необхідні для розуміння можливостей застосування мережі Інтернет і IP-протоколу для передачі мовних повідомлень.

Точне визначення терміну Інтернет було дано в жовтні 1995 р. федеральною Мережевою Радою США (FNC або Federal Networking Counsil) в наступній формі:

Інтернет - це частина глобальної інформаційної системи, яка:

- логічно зв'язана унітарним адресним простором, заснованому на IP-протоколі або на його перспективних розширеннях/послідовниках;
- може підтримувати комунікації, використовуючи Transmission Control Protocol/ Internet Protocol (TCP/IP) або його розширення/послідовники і/або IP-сумісні протоколи;
- надає, використовує або робить доступним (для всіх або конфіденційно) сервіси високого рівня, засновані на комунікаціях і пов'язаній з ними інфраструктурі, тут визначеній.

Творці технології Інтернет виходили з двох основоположних міркувань:

- неможливо створити єдину фізичну мережу, яка дозволить задовольнити потреби всіх користувачів;
- користувачам потрібен універсальний спосіб для встановлення з'єднань один з одним.

В межах кожної фізичної мережі приєднані до неї комп'ютери використовують ту або іншу технологію (Ethernet, Token Ring, FDDI, ISDN, з'єднання типу крапка-крапка**,** а останнім часом до цього списку додалися мережа ATM і навіть бездротові технології). Між механізмами комунікацій, залежними від даних фізичних мереж, і прикладними системами вбудовується нове програмне забезпечення, яке забезпечує з'єднання різних фізичних мереж один з одним. При цьому деталі цього з'єднання приховані від користувачів і їм надається можливість працювати як би в одній великій фізичній мережі. Такий спосіб з'єднання в єдине ціле безлічі фізичних мереж і одержав назву технології Інтернет, на базі якої реалізована однойменна мережа Інтернет. Основний протокол, на базі якого будується мережа Інтернет, називається Інтернет-протоколом або протоколом IP.

Для з'єднання двох і більш мереж в мережі Інтернет використовуються **маршрутизатори** (routers) - комп'ютери, які фізично сполучають мережі один з одним і за допомогою спеціального програмного забезпечення передають пакети з однієї мережі в іншу.

Технологія Інтернет не нав'язує якоїсь певної топології міжмережевих з'єднань. Додавання нової мережі до мережі Інтернет не спричиняє за собою її під'єднування до деякої центральної крапки комутації або установці безпосередніх фізичних з'єднань з тими, що всіма вже входять в мережу Інтернет мережами. Маршрутизатор знає топологію мережі Інтернет за межами тих фізичних мереж, які він сполучає, і, грунтуючись на адресі мережі призначення, передає пакет по тому або іншому маршруту. У мережі Інтернет використовуються універсальні ідентифікатори приєднаних до неї комп'ютерів (адреси), тому будь-які дві машини мають можливість взаємодіяти один з одним. У Інтернет також повинен бути реалізований принцип незалежності призначеного для користувача інтерфейсу від фізичної мережі, тобто повинна існувати безліч способів встановлення з'єднань і передачі даних, однакових для всіх фізичних мережевих технологій.

Мережа Інтернет приховує деталі з'єднань мереж між собою, тому з погляду кінцевих користувачів і по відношенню до прикладних програм мережа Інтернет є **єдиною віртуальною мережею,** до якої приєднані всі комп'ютери -незалежно від їх реальних фізичних з'єднань (мал. 1.1). Кожен комп'ютер повинен мати програмне забезпечення -доступу до мережі Інтернет, яке дозволяє прикладним програмам використовувати мережу Інтернет як одну фізичну мережу.

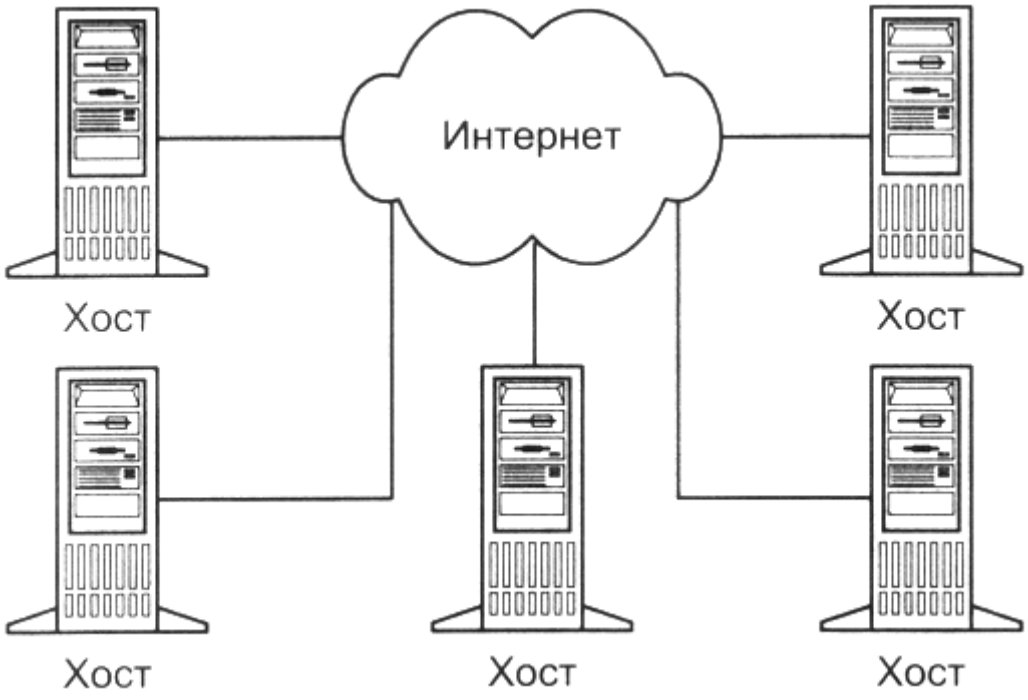


Рисунок 1.1**.** *Мережа Інтернет з погляду користувача*

Фундаментальним принципом Інтернет є рівнозначність всіх об'єднаних з її допомогою фізичних мереж: будь-яка система комунікацій розглядається як компонент Інтернет, незалежно від її фізичних параметрів, розмірів передаваних пакетів даних і географічного масштабу. На мал. 1.2 використані однакові позначення для будь-яких фізичних мереж, об'єднаних в мережу Інтернет (наприклад, з'єднань типу крапка-крапка, локальних мереж робочої групи або великих корпоративних мереж).

Універсальна мережа Інтернет будується на основі сімейства протоколів TCP/IP і включає протоколи 4-х рівнів комунікацій (мал. 1.3).

Рівень мережевого інтерфейсу відповідає за встановлення мережевого з'єднання в конкретній фізичній мережі - компоненті мережі Інтернет, до якої приєднаний комп'ютер. На цьому рівні працюють драйвер пристрою в операційній системі і відповідна мережева плата комп'ютера.

Мережевий рівень - основа стека протоколів TCP/IP. Саме на цьому рівні реалізується принцип міжмережевого з'єднання, зокрема маршрутизація пакетів по мережі Інтернет. Протокол IP - основний протокол мережевого рівня, що дозволяє реалізовувати міжмережеві з'єднання. Він використовується обома протоколами транспортного рівня - TCP і UDP. Протокол IP визначає базову одиницю передачі даних в мережі Інтернет - IP-дейтаграму, указуючи точний формат всієї інформації, що проходить по мережі TCP/IP. Програмне забезпечення рівня IP виконує функції маршрутизації, вибираючи шлях даних по з'єднаннях фізичних мереж. Для визначення маршруту підтримуються спеціальні таблиці; вибір здійснюється на основі адреси мережі, до якої підключений комп'ютер-адресат. Протокол IP визначає маршрут окремо для кожного пакету даних, не гарантуючи надійної доставки в потрібному порядку. Він задає безпосереднє відображення даних на ніжележащий фізичний рівень передачі і реалізує тим самим високоефективну доставку пакетів.

Фундаментальним принципом Інтернет є рівнозначність всіх об'єднаних з її допомогою фізичних мереж: будь-яка система комунікацій розглядається як компонент Інтернет, незалежно від її фізичних параметрів, розмірів передаваних пакетів даних і географічного масштабу. На мал. 1.2 використані однакові позначення для будь-яких фізичних мереж, об'єднаних в мережу Інтернет (наприклад, з'єднань типу крапка-крапка, локальних мереж робочої групи або великих корпоративних мереж).

Універсальна мережа Інтернет будується на основі сімейства протоколів TCP/IP і включає протоколи 4-х рівнів комунікацій (мал. 1.3).

Рівень мережевого інтерфейсу відповідає за встановлення мережевого з'єднання в конкретній фізичній мережі - компоненті мережі Інтернет, до якої приєднаний комп'ютер. На цьому рівні працюють драйвер пристрою в операційній системі і відповідна мережева плата комп'ютера.

Мережевий рівень - основа стека протоколів TCP/IP. Саме на цьому рівні реалізується принцип міжмережевого з'єднання, зокрема маршрутизація пакетів

по мережі Інтернет. Протокол IP - основний протокол мережевого рівня, що дозволяє реалізовувати міжмережеві з'єднання. Він використовується обома протоколами транспортного рівня - TCP і UDP. Протокол IP визначає базову одиницю передачі даних в мережі Інтернет - IP-дейтаграмму, указуючи точний формат всієї інформації, що проходить по мережі TCP/IP. Програмне забезпечення рівня IP виконує функції маршрутизації, вибираючи шлях даних по з'єднаннях фізичних мереж. Для визначення маршруту підтримуються спеціальні таблиці; вибір здійснюється на основі адреси мережі, до якої підключений комп'ютер-адресат. Протокол IP визначає маршрут окремо для кожного пакету даних, не гарантуючи надійної доставки в потрібному порядку. Він задає безпосереднє відображення даних на ніжележащий фізичний рівень передачі і реалізує тим самим високоефективну доставку пакетів.

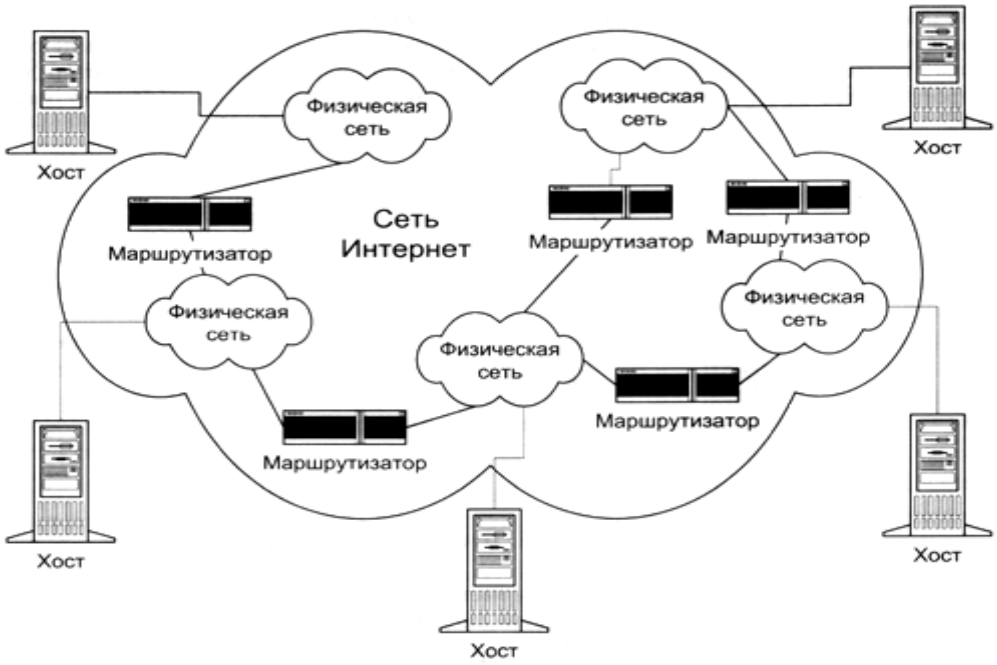


Рисунок 1.2. *Внутренняя структура сети Интернет*

Прикладний:	Telnet, FTP, E-mail і т.д.
Транспортний:	TCP, UDP
Мережевий:	IP, ICMP, IGMP
Мережевий інтерфейс:	драйвер пристрою і мережева плата

Рисунок 1.3. *Чотири рівні стека протоколів TCP / IP*

На мережевому рівні протокол IP реалізує ненадійну службу доставки пакетів по мережі від системи до системи без встановлення з'єднання (connectionless packet delivery service). Це означає, що буде виконане все необхідне для доставки пакетів, проте ця доставка не гарантується. Пакети можуть бути втрачені, передані в неправильному порядку, продубльовані і т.д. Протокол IP не забезпечує надійності комунікації. Не є механізму підтверджень ні між відправником і одержувачем, ні між хост-комп'ютерами. Не є контролю помилок для поля даних, тільки контрольна сума для заголовка. Не підтримується повторна передача, немає управління потоком. Виявлені помилки можуть оповістити за допомогою протоколу ICMP (Internet Control Message Protocol).

Надійну передачу даних реалізує наступний рівень, **транспортний,** на якому два основні протоколи, TCP і UDP, здійснюють зв'язок між машиною - відправником пакетів і машиною-адресатом.

Нарешті, **прикладний рівень** - це додатки типу клієнт-сервер, що базуються на протоколах нижніх рівнів. На відміну від протоколів решти трьох рівнів, протоколи прикладного рівня займаються деталями конкретного додатку і не цікавляться способами передачі даних по мережі. Серед основних додатків TCP/IP, наявних практично в кожній його реалізації, - протокол емуляції терміналу Telnet, протокол передачі файлів FTP, протокол електронної пошти SMTP, протокол управління мережею SNMP, використовуваний в системі World Wide Web (WWW) протокол передачі гіпертексту HTTP і ін.

Оскільки в Інтернет деталі фізичних з'єднань приховані від додатків, прикладний рівень абсолютно не піклується про те, що клієнт додатку працює в мережі Ethernet, а сервер підключений до мережі Token Ring. Між кінцевими системами може бути декілька десятків маршрутизаторів і безліч проміжних фізичних мереж різних типів, але додаток сприйматиме цей конгломерат як єдину фізичну мережу. Це і обумовлює основну силу і привабливість технології Інтернет і протоколу IP.

На базі протоколу IP будується не тільки мережа Інтернет, але і будь-які інші мережі передачі даних (локальні, корпоративні), які можуть мати або не мати вихід на глобальну мережу Інтернет. Універсальність і гнучкість мереж на базі протоколу IP дає можливість застосовувати їх не тільки для передачі даних, але і іншої мультимедійної інформації. З недавніх пір IP-мережі стали використовувати для передачі мовних повідомлень. А ось як це відбувається і буде розглянуто в даній книзі.

1.2.Визначення IP-телефонии

У технічній літературі використовуються три основні терміни для позначення технології передачі мови по мережах з пакетною комутацією на базі протоколу IP (Internet Protocol):

IP-телефонія (IP Telephony);

голос по IP-мережах (Voice over IP - VoIP);

Інтернет-телефонія (Internet Telephony).

Під **IP-телефонією** будемо розуміти технологію, що дозволяє використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP (наприклад, мережа Інтернет) як засіб організації і ведення міжнародних, міжміських і місцевих телефонних розмов і передачі факсів в режимі реального часу. За кордоном технологія передачі голосової інформації з використанням протоколу IP має сталу назву **Voice over IP (VoIP).** Відносно сервісів і технологій між IP-телефонією і VoIP немає ніякої різниці. Різні виробники можуть віддавати перевагу одному або іншому терміну або використовувати їх в рівній мірі. З точки ж зору мережевих рішень IP-телефонія, безумовно, - термін змістовніший, оскільки вона реалізується не тільки на рівні каналів передачі (як глобальних, так і локальних), але і на рівні абонентського устаткування і, що важливо, учрежденческіх автоматичних телефонних станцій (УАТС). Останнє дійсно означає фактичну інтеграцію телефонії в її звичному розумінні і IP-мереж.

Інтернет-телефонія - це окремий випадок IP-телефонії, коли як канали передачі пакетів телефонного трафіку або від абонента до оператора, або на магістралі (або на обох названих ділянках) використовуються звичайні канали мережі Інтернет.

Існують два протилежні погляди на IP-телефонію:

IP-телефонія - явище аналогічне зворотному виклику (call-back) і маршрутизації за найменшою вартістю. У цьому сенсі вона представляє загрозу для операторів традиційної телефонії, оскільки використовує їх мережеві ресурси в обхід системи міжнародних розрахунків і, отже, її потрібно заборонити за всяку ціну;

IP-телефонія - це майбутнє мережі загального користування і, отже, її потрібно всемірно підтримувати і розвивати.

Але навіть при другому підході виникли суперечності у визначеннях: IP-телефонія -ця послуга реального або нереального часу? У деяких країнах для розділення послуг телефонної мережі загального користування (ТФОП) і IP-телефонії використовуються поняття: затримка і якість обслуговування. І звідси можливі два підходи до визначення IP-телефонії:

IP-телефонія - це самостійна послуга з передачі голосу, що є дешевшою альтернативою традиційної телефонії;

IP-телефонія - найбільш проста для реалізації послуга з пакету послуг, включаючи передачу даних і відео по протоколу IP. Більш того, передача голосу - не найзначніша складова цього пакету послуг. IP-телефонія сприятиме повсюдному розповсюдженню електронної торгівлі і додавати в інтерактивні мережеві ігри або chat елемент живого спілкування.

1.3. Принципи пакетної передачі мови

Класичні телефонні мережі засновані на технології комутації каналів (мал. 1.4), яка для кожної телефонної розмови вимагає виділеного фізичного з'єднання. Отже, одна телефонна розмова є одним фізичним з'єднанням телефонних каналів. В цьому випадку аналоговий сигнал вширшки 3,1 кГц передається на найближчу АТС, де він мультіплексується за технологією тимчасового розділення з

сигналами, які поступають від інших абонентів, підключених до цієї АТС. Далі груповий сигнал передається по мережі міжстанційних каналів. Досягнувши АТС призначення, сигнал демультіплексується і доходить до адресата. Основним недоліком телефонних мереж з комутацією каналів є неефективне використання смуги каналу - під час пауз в мові канал не несе ніякого корисного навантаження.

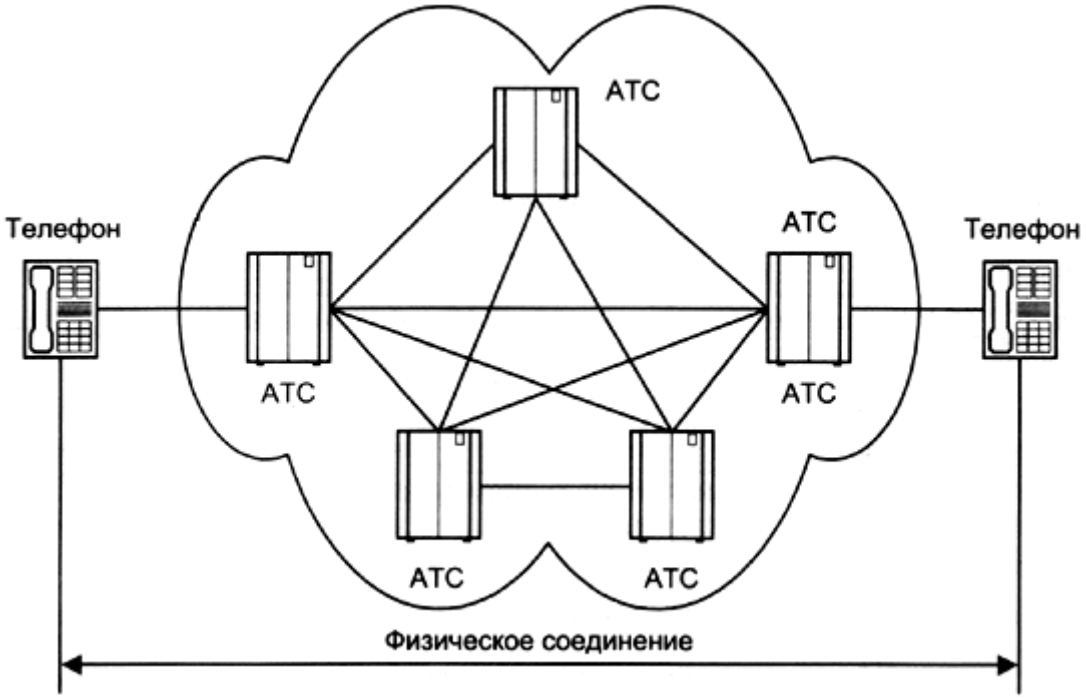


Рисунок 1.4. *З'єднання в класичній телефонній мережі*

Перехід від аналогових до цифрових технологій став важливим кроком для виникнення сучасних цифрових телекомунікаційних мереж. Одним з таких кроків в розвитку цифрової телефонії став перехід до пакетної комутації. У мережах пакетної комутації по каналах зв'язку передаються одиниці інформації, які не залежать від фізичного носія. Такими одиницями можуть бути пакети, кадри або осередки (залежно від протоколу), але у будь-якому випадку вони передаються по мережі (мал. 1.5), що розділяється, більш того - по окремих віртуальних каналах, не залежних від фізичного середовища. Кожен пакет ідентифікується заголовком, який може містити інформацію про використовуваний їм канал, його походження (тобто про джерело або відправника) і пункт призначення (про одержувача або приймач).

У мережах на основі протоколу IP всі дані - голос, текст, відео, комп'ютерні програми або інформація в будь-якій іншій формі - передаються у вигляді пакетів. Будь-який комп'ютер і термінал такої мережі має свою унікальну IP-адресу, і передавані пакети маршрутізуються до одержувача відповідно до цієї адреси, указуваної в заголовку. Дані

можуть передаватися одночасно між багатьма користувачами і процесами по одній і тій же лінії. При виникненні проблем IP-мережі можуть змінювати маршрут для обходу несправних ділянок. При цьому протокол IP не вимагає виділеного каналу для сигналізації.

Процес передачі голосу по IP-мережі складається з декількох етапів.

На першому етапі здійснюється оцифровка голосу. Потім оцифровані дані аналізуються і обробляються з метою зменшення фізичного об'єму даних, що передаються одержувачу. Як правило, на цьому етапі відбувається придушення непотрібних пауз і фонового шуму, а також компресування.

На наступному етапі одержана послідовність даних розбивається на пакети і до неї додається протокольна інформація - адреса одержувача, порядковий номер пакету на випадок, якщо вони будуть доставлені не послідовно, і додаткові дані для корекції помилок. При цьому відбувається тимчасове накопичення необхідної кількості даних для утворення пакету до його безпосередньої відправки в мережу.

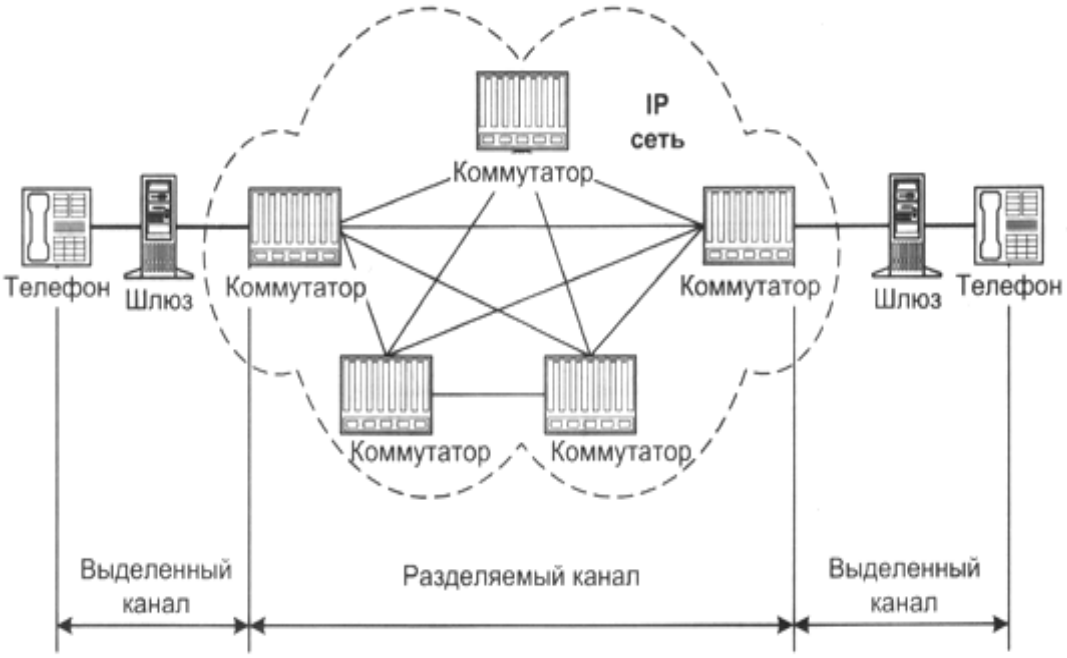


Рисунок 1.5. *З'єднання в мережі з комутацією пакетів*

Витягання переданої голосової інформації з одержаних пакетів також відбувається у декілька етапів. Коли голосові пакети приходять на термінал одержувача, то спочатку перевіряється їх порядкова послідовність. Оскільки IP-мережі не гарантують час доставки, то пакети із старшими порядковими номерами можуть прийти раніше, більш того, інтервал часу отримання також може коливатися. Для відновлення початкової послідовності і синхронізації відбувається тимчасове накопичення пакетів. Проте деякі пакети можуть бути

взагалі втрачені при доставці, або затримка їх доставки перевищує допустимий розкид. У звичайних умовах приймальний термінал запрошує повторну передачу помилкових або втрачених даних. Але передача голосу дуже критична до часу доставки, тому в цьому випадку або включається алгоритм апроксимації, що дозволяє на основі одержаних пакетів приблизно відновити втрачені, або ці втрати просто ігноруються, а пропуски заповнюються даними випадковим чином.

Одержана таким чином (не відновлена!) послідовність даних декомпресується і перетвориться безпосередньо в аудіо-сигнал, що несе голосову інформацію одержувачу.

Таким чином, з великим ступенем вірогідності, одержана інформація не відповідає початковій (спотворена) і затримана (обробка на сторонах, що передають і приймальній, вимагає проміжного накопичення). Проте в деяких межах надмірність голосової інформації дозволяє миритися з такими втратами.

Оператори мереж з пакетною комутацією одержують переваги, властиві інфраструктурі, що розділяється, електрозв'язки по самої її природі. Простіше кажучи, вони можуть продати більше, ніж насправді мають, грунтуючись на статистичному аналізі роботи мережі. Оскільки передбачається, що абоненти цілодобово і щодня не задіюватимуть всю сплачену смугу, можна обслужити більше абонентів, не розширюючи магістральну інфраструктуру. Оборот і прибуток при цьому збільшуються.

Іншими словами, абонент, що сплатив смугу 64 кбит/с, використовує канал в середньому лише на 25%. Отже, оператор здатний продати ресурс, що є у нього, в чотири рази більшому числу користувачів, не перенавантажуючи свою мережу. Такий сценарій вигідний обом сторонам - і .клієнту, і продавцю, - оскільки оператор збільшує свої доходи і зменшує абонентську платню за рахунок зниження витрат. Це виграшне рішення вже визнане в світі передачі даних, а зараз починає використовуватися і на ринку телефонії.

У теперішній час в IP-телефонії існує два основні способи передачі голосових пакетів по IP-мережі:

через глобальну мережу Інтернет (Інтернет-телефонія);

використовуючи мережі передачі даних на базі виділених каналів (IP-телефонія).

У Першому випадку смуга пропускання безпосередньо залежить від завантаженості мережі Інтернет пакетами, що містять дані, голос, графіку і т.д., а значить, затримки при проходженні пакетів можуть бути самими різними. При використанні виділених каналів виключно для голосових пакетів можна гарантувати фіксовану (або майже фіксовану) швидкість передачі. Зважаючи на широке розповсюдження мережі Інтернет особливий інтерес викликає реалізація системи Інтернет-телефонії, хоча слід визнати, що в цьому випадку якість телефонного зв'язку оператором не гарантується.

Для того, щоб здійснити міжміський (міжнародну) зв'язок за допомогою телефонних серверів, організація або оператор послуги повинні мати по серверу в

тих місцях, куди і звідки плануються дзвінки. Вартість такого зв'язку на порядок менше вартості телефонного дзвінка по звичайних телефонних лініях. Особливо велика ця різниця для міжнародних переговорів.

Загальний принцип дії телефонних серверів Інтернет-телефонії такий: з одного боку, сервер пов'язаний з телефонними лініями і може з'єднатися з будь-яким телефоном миру. З іншого боку, сервер пов'язаний з Інтернетом і може зв'язатися з будь-яким комп'ютером в світі. Сервер приймає стандартний телефонний сигнал, оцифровує його (якщо він початково не цифровий), значно стискає, розбиває на пакети і відправляє через Інтернет за призначенням з використанням протоколу IP. Для пакетів, що приходять з мережі на телефонний сервер і що йдуть в телефонну лінію, операція відбувається в зворотному порядку. Обидві операції (вхід сигналу в телефонну мережу і його вихід з телефонної мережі), що становлять, відбуваються практично одночасно, що дозволяє забезпечити повнодуплексну розмову. На основі цих базових операцій можна побудувати багато різних конфігурацій. Наприклад, дзвінок телефон-комп'ютер або комп'ютер-телефон може забезпечувати один телефонний сервер. Для організації зв'язку телефон (факс) -телефон (факс) потрібні два сервери.

Основним стримуючим чинником на шляху масштабного впровадження IP-телефонії є відсутність в протоколі IP механізмів забезпечення гарантованої якості послуг, що робить його поки не найнадійнішим транспортом для передачі голосового трафіку. Сам протокол IP не гарантує доставку пакетів, а також час їх доставки, що викликає такі проблеми, як рваний голос і просто провали в розмові. Сьогодні ці проблеми розв'язуються: організації по стандартизації розробляють нові протоколи, виробники випускають нове устаткування, але на цьому рівні справи з сумісністю і стандартизацією йдуть вже не так добре, як з упаковкою мови в пакети. Помітимо, що якщо в рамках приватної корпоративної мережі деяка втрата якості голосового зв'язку при сильній завантаженості ресурсів цілком терпима за умови, що середній показник буде цілком задовільним, то у разі мережі загального користування все набагато серйозніше.

Оскільки оператор надає деякий сервіс і бере за нього гроші, він зобов'язаний гарантувати його якість. Навіть якщо клієнт згоден (хоча в умовах жорсткої конкуренції на ринку телекомунікацій це маловірогідно) час від часу миритися з не дуже високим рівнем якості, він може пред'явити претензії у разі серйозних або тривалих проблем. Як би там не було, оператор вимушений стежити за якістю послуг, що надаються, для чого у разі їх масштабного надання йому потрібна відповідна апаратура і програмне забезпечення, яке достатньо дорого коштує і є не в усіх точках мережі.

З погляду масштабності (якщо відвернутися від проблем з неконтрольованим погіршенням якості при зростанні навантаження на мережу) IP-телефонія представляється цілком закінченим рішенням. По-перше, оскільки з'єднання на базі протоколу IP може починатися (і закінчуватися) в будь-якій точці мережі від абонента до магістралі. Відповідно, IP-телефонію в мережі можна вводити ділянку за ділянкою, що, до речі, на руку і з погляду міграції, оскільки її можна

проводити зверху вниз, від низу до верху або по будь-якій іншій схемі. Для вирішень IP-телефонії характерна певна модульна: кількість і потужність різних вузлів - шлюзів, gatekeeper (сторожів - так в термінології VoIP іменуються сервери обробки номерних планів) - можна нарощувати практично незалежно, відповідно до поточних потреб. Природньо, проблеми нарощування ресурсів власне мережевої інфраструктури ми зараз не враховуємо, оскільки вузли самої мережі можуть бути незалежні від системи IP-телефонії, а можуть і суміщати в собі їх функції.

Прогрес впровадження технології IP-телефонії характеризують наступні цифри. У 1996 році IP-телефонія за один рік виросла на 997% (від оціненого в 1.8 мільйонів дол. ринку), але в 1997 р. об'єм ринку устаткування, програмного забезпечення і послуг IP-телефонії оцінений вже в 210 млн. дол. Доходи від надання послуг телефонного і факсимільного зв'язку в IP-мережах склали 123 млн. дол. Хоча голосовий трафік IP-телефонії складає менше 1% від всіх міжміських і міжнародних дзвінків, ринок Інтернет-телефонії в 1999 році досяг 560 мільйонів дол.

Варто згадати про деякі прогнози розвитку ринку IP-телефонії. Їх роблять багато відомих аналітичних компаній. Прогнози здебільшого оптимістичні, але звучать і голоси песимістів.

Так, експерти компанії Killen&Associates припускають 138% щорічного приросту ринку до 2002 р., а експерти Frost&Sullivan орієнтуються на 149%. Аналітики Philips Group-lnfoTech прогнозують в 2004 р. досягнення цим сегментом ринку рівня 1,9 млрд. дол. (при загальному об'ємі ринку устаткування телефонних систем в 16 млрд. дол.).

За прогнозами компанії Yankie Group, частка міжміських і міжнародних дзвінків (за часом), здійснюваних по IP-мережах, має велику тенденцію зростання і досягне, наприклад, в США до 2005 р. 15% (мал. 1.6).

В той же час, за оцінками компанії TeleChoice, що співробітничає з фірмою Lucent Technologies у області VoIP, зараз ринок IP-телефонії складає всього 0,1% від спільного ринку мовних послуг. За прогнозами цієї компанії, через п'ять років частка ринку IP-телефонії зросте всього лише до 2%. За прогнозом експертів дослідницької компанії Insight Research навіть північноамериканський ринок пакетної телефонії в 2004 р. складе лише 10% обороту ринку послуг телефонного зв'язку. Слід підкреслити, що під пакетною телефонією експерти Insight Research розуміли не тільки технологію IP-телефонії, але транспортування голосу за допомогою фреймів Frame Relay (VoFR) і осередків ATM (VoATM).

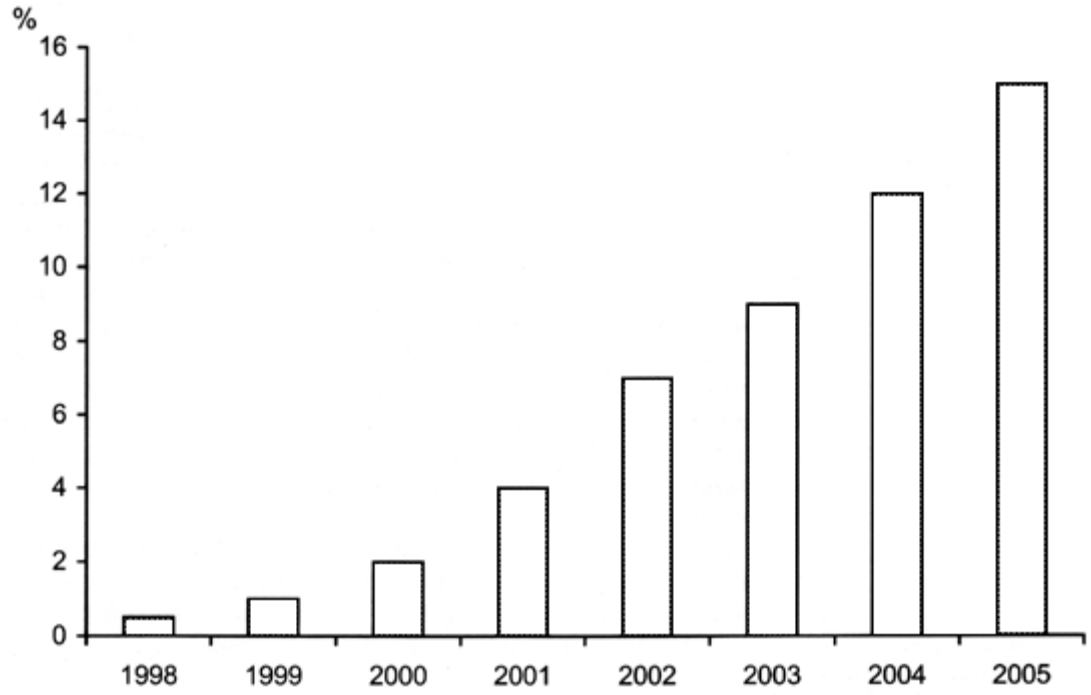


Рисунок 1.6. *Стан і прогноз частки трафіку IP-телефонії в США (за даними фірми Yankie Group)*

За даними фірми Killen & Associates, голосовий трафік IP-телефонії в 1998 році в компаніях, що входять в список Fortune 1000, складав менше 1% від всіх міжміських і міжнародних дзвінків. Крім того, за оцінками фірм IDC, Link Research навіть в 2001 році об'єм передачі голосу в мережах з комутацією пакетів складе в США: міжнародні дзвінки з території США - 4 млрд. хвилин; дзвінки в межах США - 8,5 млрд. хвилин. Це складатиме 0,98% (менше одного відсотка) загального об'єму внутрішнього (в межах США) і міжнародного трафіку. Згідно з даними Datamonitor, частка IP-телефонії в загальних доходах телефонних компаній в США і Європі поки що дуже мала і навіть в перспективі не перевищить 1% (мал. 1.7).

Незалежно від приведених прогнозів з упевненістю можна сказати, що IP-телефонія найближчим часом не стане повноцінною альтернативою традиційної телефонії, але зможе зайняти певне місце особливо в корпоративному сегменті, де повною мірою проявить свою дійсну перевагу - можливість супроводу телефонними переговорами потоку даних в єдиному каналі зв'язку. Сеанси одночасної роботи з однією і тією ж інформацією в корпоративних мережах, відеоконференції, Інтернет-комерція в режимі он-лайн - ось де IP-телефонія поза сумнівом займе гідне положення навіть із зниженою якістю мови, оскільки основне смислове навантаження в цих випадках нестиме інформація на дисплеї комп'ютера або відеоекрані. При цьому повністю використовуються переваги мультимедійного зв'язку: оперативність і ефективність ділового спілкування, економія канальних ресурсів і часу. При цьому IP-телефонія виступає як допоміжний засіб комунікації, доповнюючий передачу даних, відеозображень, WEB-сторінок.

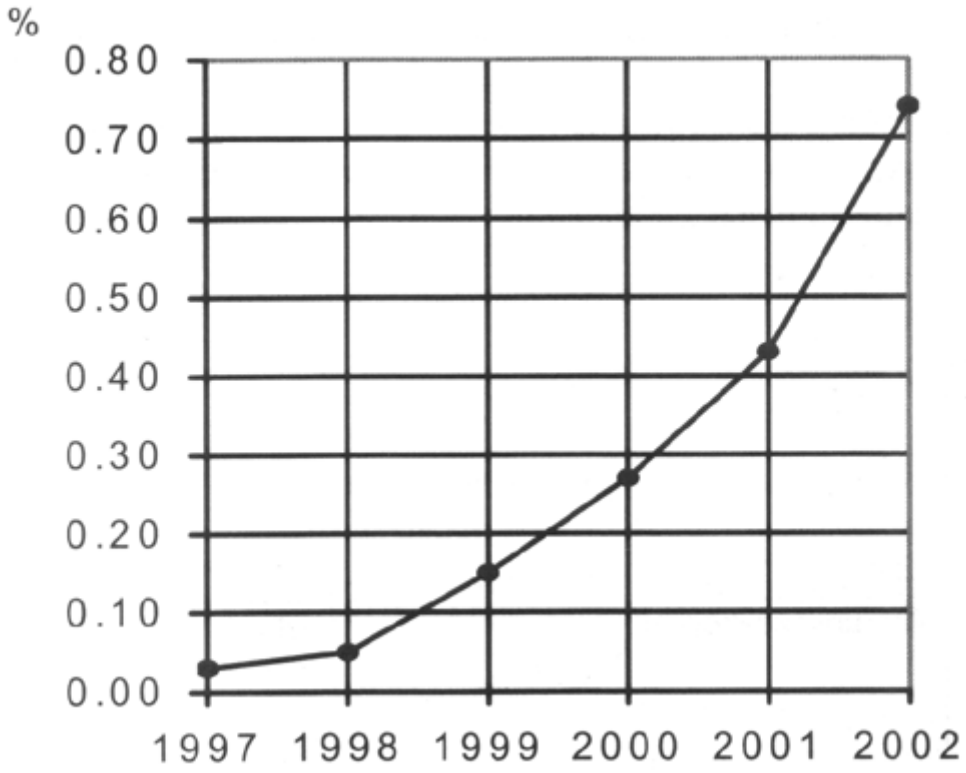


Рисунок 1.7. *Частка IP-телефонії в загальних доходах телефонних компаній в США і Європі % (за даними Datamonitor)*

1.4. Види з'єднань в мережі IP-телефонії

Мережі IP-телефонії надають можливості для викликів чотирьох основних типів:

- Від телефону до телефону (мал. 1.8). Виклик йде із звичайного телефонного апарату до АТС, на один з виходів якої підключений шлюз IP-телефонії, і через IP-мережу доходить до іншого шлюзу, який здійснює зворотні перетворення.
- Від комп'ютера до телефону (мал. 1.9). Мультимедійний комп'ютер, що має програмне забезпечення IP-телефонії, звукову плату (адаптер), мікрофон і акустичні системи, підключається до IP-мережі або до мережі Інтернет, і з іншого боку шлюз IP-телефонії має з'єднання через АТС із звичайним телефонним апаратом.

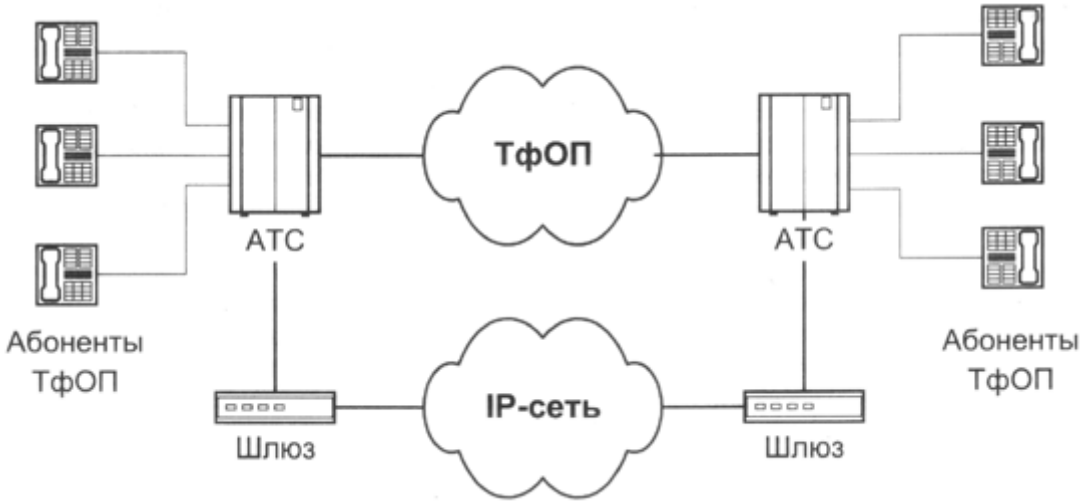


Рисунок 1.8. *Схема зв'язку телефон-телефон*

Слід зазначити, що в з'єднаннях 1 і 2 тип замість телефонних апаратів можуть бути включені апарати, факсиміле, і в цьому випадку мережа IP-телефонії повинна забезпечувати передачу повідомлень, факсиміле.

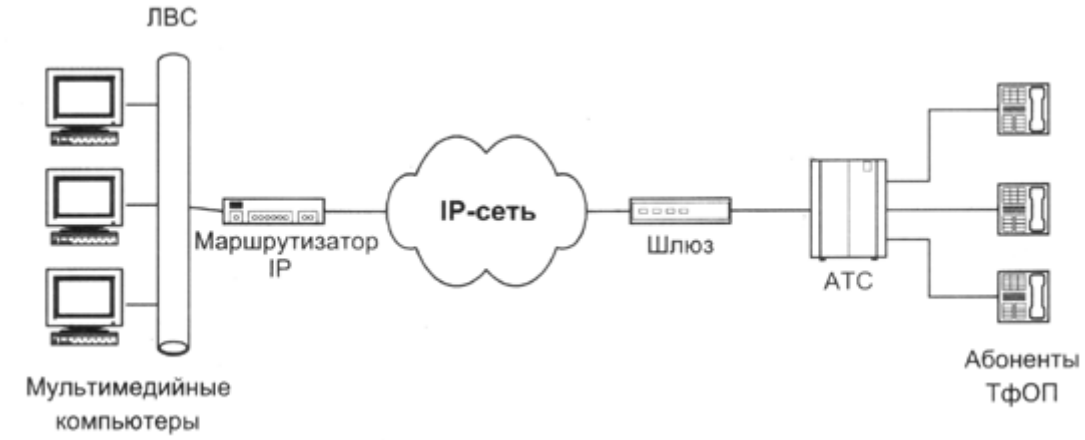


Рисунок 1.9. *Схема зв'язку комп'ютер-телефон*

3. Від комп'ютера до комп'ютера (мал. 1.10). В цьому випадку з'єднання встановлюється через IP-мережу між двома мультимедійними комп'ютерами, обладнаними апаратними і програмними засобами для роботи з IP-телефонією.

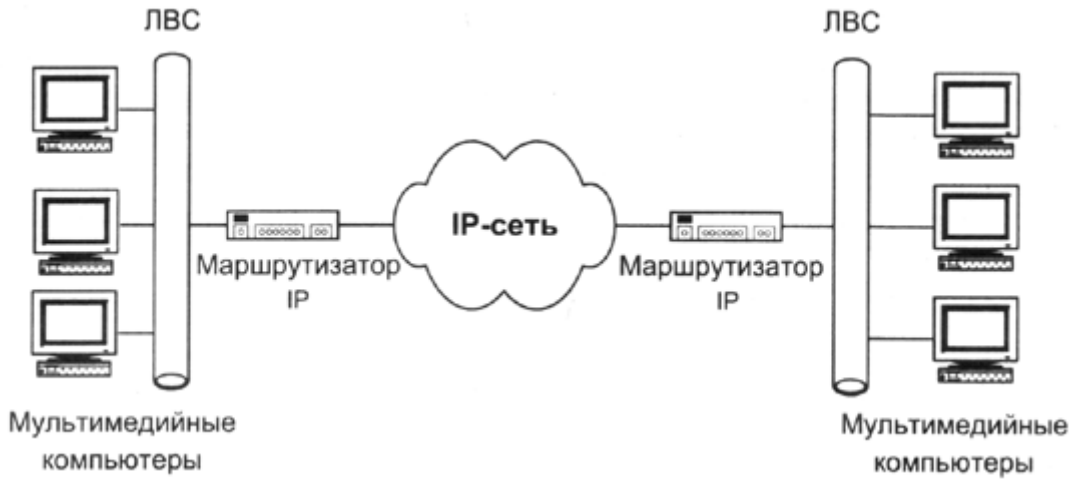


Рисунок 1.10. *Схема зв'язку комп'ютер-комп'ютер*

1.5. Переваги використання IP-телефонії

Кінцевий користувач IP-телефонії не тільки збереже наявні переваги телефонної мережі загального користування, які включають широкий діапазон послуг, простоту використання, надійність і якість голосу, але і одержить наступні додаткові переваги:

- нижчі ціни на традиційні послуги телефонного зв'язку;
- IP-телефонія одночасно підтримує голос і дані, задовольняючи вимогам конвергенції. Це означає, що клієнти одержать додаткові переваги від економії в розвитку, можливі за рахунок використання єдиної мережі, а також за рахунок того, що об'єми трафіку і шаблони швидко змінялися від даних до голосу і навпаки і це захищає клієнта;
- феноменальна мобільність користувача, яку забезпечує мережа IP-телефонії: дзвінки і факси автоматично перенаправляються в будь-яку точку миру, користувачі матимуть доступ до одного і того ж набору послуг незалежно від того, де і як вони підключаються до мережі. Ця розподілена архітектура забезпечує прекрасну гнучкість і робить можливою відсутність прив'язки до місця надання послуги;
- новий набір пристроїв доступу, від традиційних телефонів і факсів до комп'ютерів;
- доступ до нових послуг (голосова пошта, конференцзв’язок , передача факсу і ін.) через Відкритий інтерфейс архітектури па базі IP, що забезпечує сумісність для широкого спектру розробників додатків;
- можливість настройки набору послуг;
- простота оплати послуг IP-телефонії (звичайно за допомогою телефонних карток, що предоплаченных);
- простота контролю користувачем стану його розрахункового рахунку (через мережу Інтернет).

Разом з провайдерами IP-телефонії Інтернет-провайдери також можуть зайняти певну нішу на ринку послуг IP-телефонії, оскільки існуюча у них IP-інфраструктура дає хороші можливості для впровадження послуг голосового зв'язку. Необхідні для цього апаратні і програмні засоби можна встановлювати поетапно. Інтернет-провайдери вже мають крапки присутність, пов'язана з комутаторами місцевих провайдерів і операторів мережі загального користування.

Для Інтернет-провайдерів послуга Інтернет-телефонії забезпечує наступні переваги:

- заощадження капітальних вкладень за рахунок використання відкритих комп'ютерних платформ;
- зниження експлуатаційних витрат як результат надання різноманітності послуг на єдиній мережі;
- відкрите середовище розробника послуги означає більш конкурентну, а отже, менш дорогу розробку нових послуг.
- безліч послуг може бути доступно через єдиний канал з користувачем, що означає більше послуг (прибули) з розрахунку на одного користувача.

Оператори класичних телефонних мереж недовірливо віднеслися до появи IP-телефонії, оскільки передача мови по IP-мережах неминуче вимушує їх знижувати тарифи на міжміські і міжнародні розмови, що приведе до прямого скорочення їх доходів. Так, фінансові служби США обіцяють збитки найбільшого постачальника традиційного телефонного сервісу - компанії AT&T від 620 до 950 мільйонів доларів на міжнародних дзвінках від втрати частки ринку на користь засобів IP-телефонії.

З появою IP-телефонії у рядах операторів телекомунікації почалася легка паніка, яка викликала перше і цілком логічне бажання витіснити з ринку конкурентів, що з'явилися, за допомогою відомих лобістських прийомів, що дозволяють чинити тиск на національні адміністрації зв'язку з метою обмеження ліцензування, а також за допомогою підвищення платні за доступ в Інтернет. Деякі американські оператори, наприклад, намагалися добитися заборони IP-телефонії через Федеральну комісію зв'язку, проте зважаючи на потенційний утиск прав споживачів все це успіху не мало.

В результаті традиційні телефоністи вимушені були самі зайнятися IP-технологіями і, треба віддати їм належне, досить швидко досягли успіху в цьому, використовуючи IP-рішення як мінімум для створення резервних каналів для пропуску трафіку на випадок перевантажень або аварій, що дозволило одержувати їм додатковий прибуток. Одночасно в даний час проектуються універсальні магістральні IP-мережі, які в майбутньому повинні не те щоб замінити традиційні телефонні мережі, але істотно їх доповнити послугами передачі даних, відео і мультимедіа.

Тим часом виявилось, що, на жаль, IP-телефонія, не приводить до багатократної економії засобів оператора, що вкладаються в передачу голосового трафіку на дальні відстані, як це на перший погляд може показатися при аналізі

діяльності сьогоднішніх компаній, що надають ці послуги. І каменем спотикання тут є вся та ж якість передачі мови. В результаті сьогодні IP-технології з успіхом застосовуються для створення виділених мультисервисных корпоративних мереж зв'язку. Але якщо йдеться про вихід в загальнодоступний Інтернет, в якому працюють мільйони користувачів, - гарантувати високу якість передачі мовного трафіку не береться ніхто. Адже передача мови вельми чутлива до затримок, а Інтернет зовсім не гарантує не те що затримку, але просту доставку всіх посланих IP-пакетів, які можуть приходити в пункт призначення різними шляхами і зовсім не в тому порядку, в якому посилалися. І те, що звичайному користувачу Інтернету, що бродить по Web-сайтах, деколи непомітно, користувачу Інтернет-телефонії дуже навіть заважає.

Крупних телекомунікаційних операторів, обслуговуючих тисячі і сотні тисяч клієнтів, вимушені вкладати для досягнення якості, гідного їх імені, такі засоби, які мало поступаються інвестиціям для створення традиційної мережевої інфраструктури. Мовний трафік безлічі абонентів потрібно десь зібрати, перетворити його в пакети даних, передати в потрібний регіон по IP-мережі і, перетворивши назад в початковий вигляд, подати в місцеву телефонну мережу загального користування (ТФОП). Для гарантії якості замість каналів загальнодоступного Інтернету потрібні виділені магістральні канали (хоч і ущільнені за допомогою технології IP-телефонії) у всі необхідні регіони і країни, потрібна могутніша місцева телефонна мережа в місцях установки шлюзу або потрібна установка декількох шлюзів (для цього потрібно вкладати в місцеву ТФОП відповідні інвестиції) і багато що інше. Саме так і працюють сьогодні серйозні постачальники послуг IP-телефонії. Таким чином, для крупних операторів IP-телефонія сьогодні - це спосіб ефективніше використовувати існуючий мережевий ресурс і можливість надання своїм клієнтам сучасного спектру додаткових послуг (голосова пошта, конференцзв’язок, пошук номерів, ОСьконтроль за розрахунками і багато що інше), які не реалізовані в традиційній телефонній мережі, і за рахунок яких оператор може одержати додатковий прибуток.

Тому, не дивлячись на те, що має сьогодні в світі місце перевищення об'ємів трафіку даних над об'ємами голосового трафіку найближчими роками не очікується яких-небудь революційних змін, наприклад, як повне витіснення традиційних технологій передачі голосу.

2.ОСОБЛИВОСТІ ПЕРЕДАЧІ МОВНОЇ ІНФОРМАЦІЇ ЧЕРЕЗ IP-МЕРЕЖІ.

2.1. Затримки в IP-мережах.

При передачі мови по IP-мережі виникають набагато більші затримки ніж в ТМЗК. Ці затримки мають цілком випадковий характер. Є кілька основних причин виникнення затримок. По-перше це *вплив мережі.* Якщо завантаження мережі незначне, маршрутизатори та комутатори опрацьовують пакети практично миттєво, але при зростанні навантаження черги на опрацювання зростають, що й стає причиною затримок. Чим більше маршрутизаторів та комутаторів стоїть на шляху пакета до кінцевої точки, тим більший час запізнення, та більша варіація цього часу, тобто джиттер.

Ще одним джерелом затримок є *операційна система*. Більшість сучасних операційних систем не можуть контролювати розподіл часу центрального процесора, між різними процесами з точністю, більше декількох десятків мілісекунд. Щоб мінімізувати вплив ОС деякі виробники шлюзів IP-телефонії використовують ОС реального часу (VxWorks, pSOS, QNX, Neutrino). Ще одним рішенням проблеми тут може служити використання спеціалізованого процесора, який обробляв би мовну інформацію не завантажуючи центральний процесор.

Третьою причиною затримок може стати *кодек*. Оскільки більшість сучасних алгоритмів кодування орієнтовані на пакетну передачу відліків, це в свою чергу веде до певної, хоч і невеликої, затримки. Тим більше, що для ефективної роботи кодеку потрібно аналізувати інформацію, що надходить, об’єм якої перевищує об’єм одного пакета.

2.2. Вимоги до IP-мереж.

Закодована мовна інформація генеруються з заданою (не обов'язково фіксованою) швидкістю незалежно від завантаження мережі. Потрібно, щоб інформація була доставлена одержувачу з точно тією же швидкістю, з якою її генерував відправник. Передача такої інформації як аудіо, відео, синхронні потоки сама по собі не вимагає дуже малої затримки між джерелом і приймачем. Однак принципово необхідно, щоб затримка була передбачувана, тому що тільки в цьому випадку часові параметри переданих повідомлень можуть бути відновлені в приймачі.

Вимоги до швидкості передачі інформації для різних послуг варіюються дуже широко. Наприклад, передача даних телеметрії в реальному часі може вимагати швидкості в декілька біт/с, для мовної інформації задовільної якості буде потрібно від 4 до 32 Кбіт/с, для забезпечення якості на рівні ТМЗК необхідно до 64 Кбіт/с, передача відео вимагає від десятків Кбіт/с до десятків Мбіт/с (HDTV), у залежності від характеристик системи (розмір зображення, частота кадрів, спосіб кодування і т.д.). Вимоги до часу доставки теж можуть бути різні. Наприклад, при

організації мовного зв'язку допускається наскрізна затримка від 12 мс при відсутності эхокомпенсації (G.164), і до 400 мс при її наявності.

Процес передачі даних по мережах з комутацією пакетів піддається впливу статистично змінної затримки (джиттера), що виникає при обробці черг у вузлах мережі. Джиттер компенсується приймачем шляхом використання буфера відтворення. Приймач повинен мати інформацію про статистичні характеристики затримки, щоб передбачити необхідне місце в буфері.

Мережа Інтернет була створена для передачі даних на основі адаптивної маршрутизації, що припускає ситуацію, коли дані можуть передаватись різними маршрутами, які обираються в залежності від певних умов. Крім того, у мережі Інтернет не передбачалося встановлення з'єднання між джерелом і приймачем інформації, тобто між комп'ютерами в мережі не встановлюється ніяких зв'язків. Це приводить до того, що пакети часто приходять до одержувача не в тій послідовності, у якій вони були передані.

Інтернет - мережа з доставкою в міру можливості. Це означає, що мережа намагається доставити інформацію, але якщо це в силу певних причинами не виходить, інформація буде загублена. Утрати пакетів в Інтернет носять пакетний характер, тобто усередині деяких інтервалів часу губиться відразу багато пакетів. Ця характеристика мережі Інтернет робить важчою організацію передачі мультимедійної інформації, оскільки такі додатки нормально працюють тільки в умовах випадково-незалежних втрат.

Крім того сьогодні Інтернет надає будь-яким додаткам і будь-яким користувачам однаковий рівень якості обслуговування. Це не дозволяє порівнювати якість послуг IP-телефонії з якістю послуг ТМЗК, тому що в ТМЗК існують і діють дуже тверді специфікації якості обслуговування викликів. Для рішення названої проблеми необхідно забезпечити можливість резервування ресурсів мережі в процесі встановлення з'єднань.

2.3. Забезпечення якості передачі мови в IP-телефонії.

2.3.1 Забезпечення якості передачі мови на базі протоколу RSVP.

Одним із засобів забезпечення якості IP-телефонії та особливо Інтернет-телефонії є використання протоколу резервування ресурсів (Resource Reservation Protocol, RSVP), рекомендованого комітетом IETF. З допомогою RSVP мультимедійні програми можуть вимагати спеціальної якості обслуговування (specific quality of service, QoS). Протокол RSVP забезпечує певний рівень QoS завдяки тому, що на кожному вузлі, котрий зв’язує між собою учасників розмови, заздалегідь резервується деяка частина пропускної здатності рис.1.2. Використовуючи RSVP відправник періодично інформує приймач про вільну кількість ресурсів повідомленням RSVP Path. Транзитні маршрутизатори, через які передається повідомлення Path, в свою чергу, аналізують кількість своїх вільних ресурсів, резервують частину пропускної здатності і повідомляють пре це відправника повідомленням RSVP Resv. Взагалі механізм роботи протоколу RSVP не є досконалим. При застосуванні даного протоколу можливе виникнення ряду проблем, тому на практиці використання протоколу RSVP має хороші перспективи лише на корпоративному рівні.

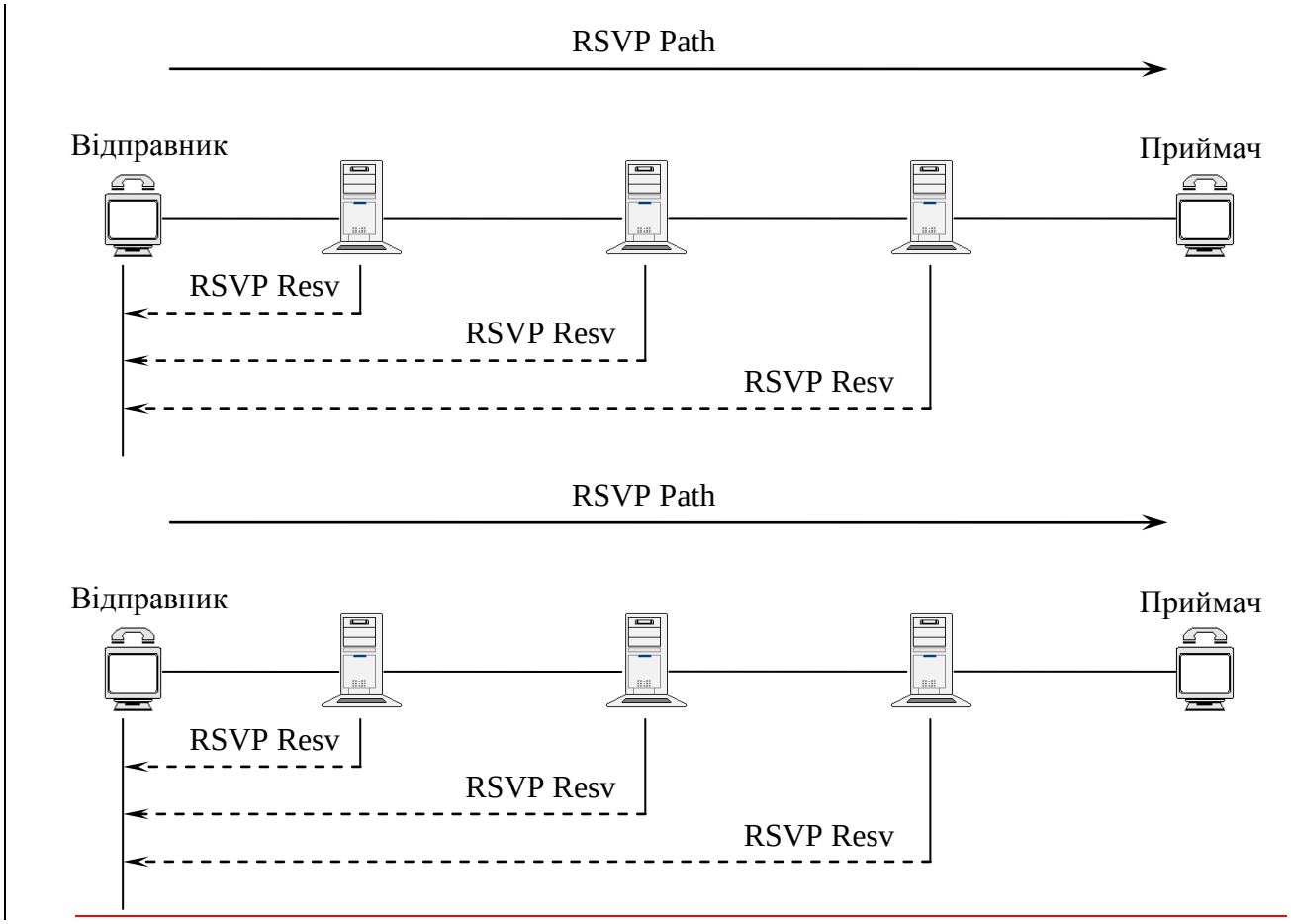


Рисунок 2.1. Робота протоколу RSVP.

2.3.2 Забезпечення якості передачі мови на базі протоколу RTP.

Компенсувати негативний вплив джиттера та затримок дозволяє розроблений IETF протокол прикладного рівня RTP (Real-time Transport Protocol), котрий використовується технологіями H.323, та SIP. Даний протокол використовується для доставки чутливої до затримок інформації. RTP не має власних механізмів, гарантуючих своєчасну доставку пакетів, – це виконують протоколи нижніх рівнів. Зазвичай протокол RTP працює поверх UDP, проте може використовувати й інші транспортні протоколи рис.1.3 Служба RTP передбачає накази типу корисного навантаження номеру пакета в потоці, а також використання часових міток. Відправник помічає кожен RTP-пакет часовою міткою, завдяки чому одержувач може вичислити сумарну затримку. Різниця в затримці пакетів дозволяє визначити джиттер, а значить зменшити його вплив – всі пакети будуть видаватися додатку з однаковою швидкістю.

Дані (аудіо, відео) Керування Резервування ресурсів

RTP	RTCP	RSVP
UDP		
IP		

Рисунок 2.2. Місце протоколів RTP, RTCP та RSVP в протокольному стеці TCP/IP.

2.3.3. Забезпечення якості передачі мови на базі протоколу RTCP.

Можливості RTP можна розширити об'єднавши його з протоколом керування передачею в реальному часі (Real-time Transport Control Protocol, RTCP), також розробленим IETF. За допомогою RTCP контролюється доставка RTP-пакетів. Основною функцією RTCP є організація зворотного зв'язку з протилежною стороною для звіту про якість прийнятої інформації. RTCP передає дані про значення джиттера, затримку, кількість переданих та втрачених пакетів. Ця інформація може бути використана передавачем для зміни параметрів передачі, наприклад для зменшення коефіцієнта стиснення інформації з метою покращення якості передачі.

На практиці вищеописані протоколи використовуються сумісно один з одним. Тільки в такому випадку можна досягти покращення якості передачі чутливої до затримок інформації.

2.3.4 Забезпечення якості передачі мови на базі диференційного обслуговування.

Технологія диференційного обслуговування (DiffServ) бере свій початок з більш ранньої технології інтегрованого обслуговування (IntServ). Проте DiffServ пропонує більш простий та масштабований метод QoS для додатків реального часу. Ключовим моментом даної технології є пере визначення поля „Тип сервісу" в заголовку IPv4. В технології DiffServ поле „DS" містить інформацію, на основі якої вузли вдовж маршруту вирішують яким саме чином опрацювати даний пакет. На даний час стандартизовані два значення поля: Default (DE) – по мірі можливості, прийняте по замовчуванню, та Expedited Forwarding (EF) – термінова відправка.

Використання технології DiffServ дає можливість класифікувати та об'єднати однотипні потоки. Весь трафік з однотипними мітками обробляється однаковим чином, що значно полегшує та пришвидшує обробку трафіку в цілому. Така перспектива робить реалізацію DiffServ, як в корпоративній так і в глобальній мережі більш реальною задачею порівняно з реалізацією його попередником IntServ. На даний час все більше виробників мережевого обладнання включає підтримку технології DiffServ в свої вироби. Це говорить тільки про те, що дана технологія насправді покращує передачу чутливої до затримок інформації через глобальні мережі, не створюючи при цьому великих накладних видатків.

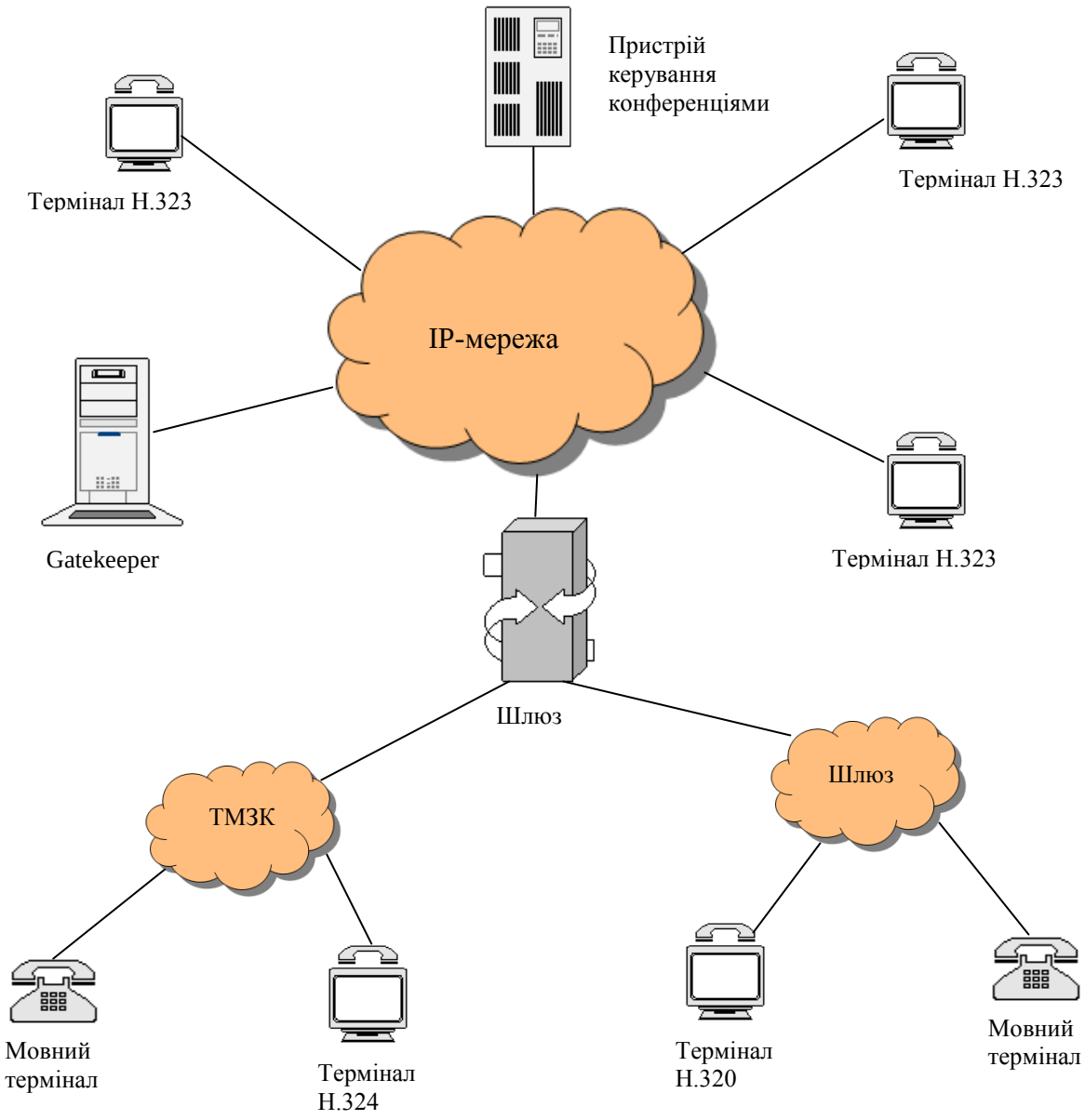
3. АНАЛІЗ ПРОТОКОЛІВ IP-ТЕЛЕФОНІЇ

3.1 Побудова мережі за рекомендацією H.323.

Перший в історії підхід до побудови мереж IP-телефонії на стандартизованій основі запропонований Міжнародним союзом електрозв'язку (ITU) у рекомендації H.323. Мережі на базі протоколів H.323 орієнтовані на інтеграцію з телефонними мережами і можуть розглядатися як мережі ISDN накладені на мережі передачі даних. Зокрема, процедура встановлення з'єднання в таких мережах IP-телефонії базується на рекомендації Q.931 та аналогічна процедурі, що використовується в мережах ISDN.

Рекомендація H.323 передбачає досить складний набір протоколів, що призначений не просто для передачі мовної інформації по IP-мережах з комутацією пакетів. Його ціль - забезпечити роботу мультимедійних додатків у мережах з негарантованою якістю обслуговування. Мовний трафік - це тільки один з додатків H.323, поряд з відеоінформацією та даними.

Варіант побудови мереж IP-телефонії, запропонований Міжнародним союзом електрозв'язку в рекомендації H.323, добре підходить тим операторам місцевих телефонних мереж, що зацікавлені у використанні мережі з комутацією пакетів для надання послуг міжміського і міжнародного зв'язку. Протокол RAS, що входить у сімейство протоколів H.323, забезпечує контроль використання мережних ресурсів, підтримує аутентифікацію користувачів і може забезпечувати нарахування плати за послуги.


Пристрій керування конференціями
Термінал H.323
Термінал H.323
IP-мережа
Gatekeeper
Термінал H.323
Шлюз
ТМЗК
Шлюз
Мовний термінал
Термінал H.324
Термінал H.320
Мовний термінал

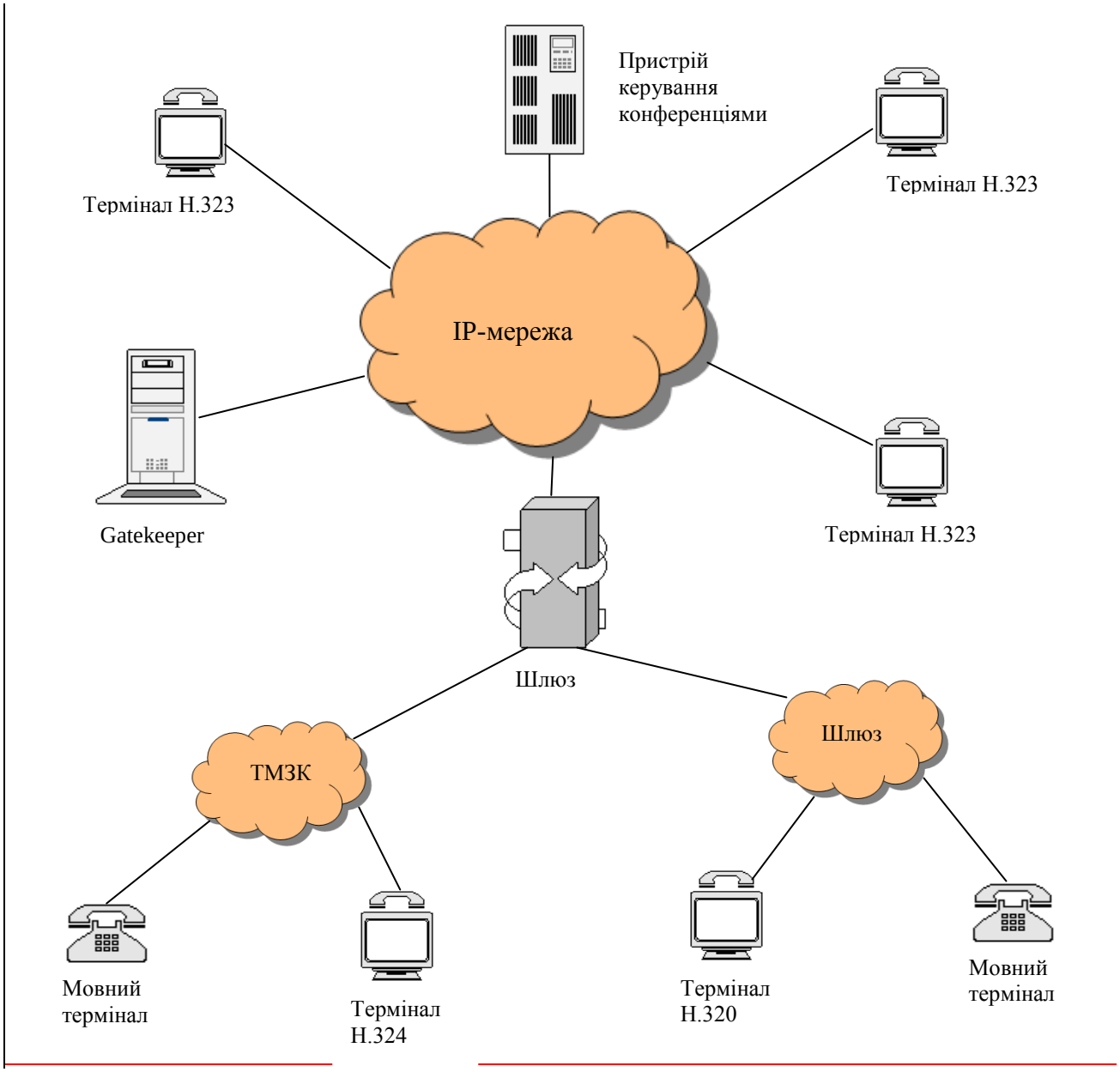


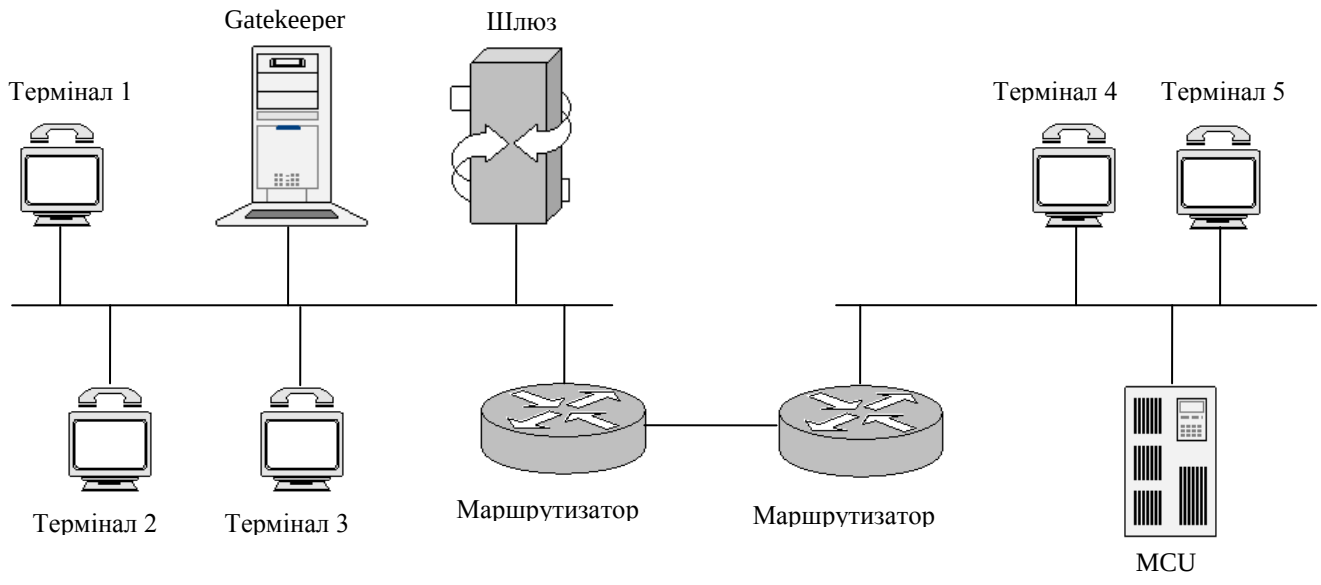
Рисунок 3.1 Архітектура мережі H.323.

На рисунку 3.1 представлена архітектура мережі на базі рекомендації H.323. Основними пристроями мережі є: термінал, шлюз, gatekeeper та пристрій керування конференціями. *Термінал* H.323 – кінцевий пристрій користувача мережі IP-телефонії який забезпечує двохсторонній мультимедійний зв'язок з іншим терміналом H.323, шлюзом чи пристроєм керування конференціями.

Шлюз IP-телефонії реалізує передачу мовного трафіка по мережах з маршрутизацією пакетів IP по протоколу H.323. Основне призначення шлюзу - перетворення мовної інформації, що надходить з боку ТМЗК, у вид, придатний для передачі по мережах з маршрутизацією пакетів IP. Крім того, шлюз перетворює сигнальні повідомлення систем сигналізації DSS1 та ЗКС7 у сигнальні повідомлення H.323 і робить зворотне перетворення відповідно до рекомендації ITU H.246.

У gatekeeper зосереджений весь інтелект мережі IP-телефонії. Мережа. побудована відповідно до рекомендації H.323, має зонну архітектуру (рис.2.2). Gatekeeper виконує функції керування однією зоною мережі IP-телефонії, у яку входять: термінали, шлюзи, пристрої керування конференціями, зареєстровані в даного gatekeeper. Окремі фрагменти зони мережі H.323 можуть бути територіально рознесені і з'єднуватися один з одним через маршрутизатори. Найбільш важливими функціями gatekeeper є:

- реєстрація кінцевих та інших пристроїв;
- контроль доступу користувачів системи до послуг IP-телефонії за допомогою сигналізації RAS;
- перетворення alias-адреси користувача (імені абонента, телефонного номера, адреси електронної пошти й ін.) у транспортну адресу мереж з маршрутизацією пакетів IP (IP адреса + номер порту TCP);
- контроль, керування і резервування пропускної здатності мережі;
- ретрансляція сигнальних повідомлень H.323 між терміналами.



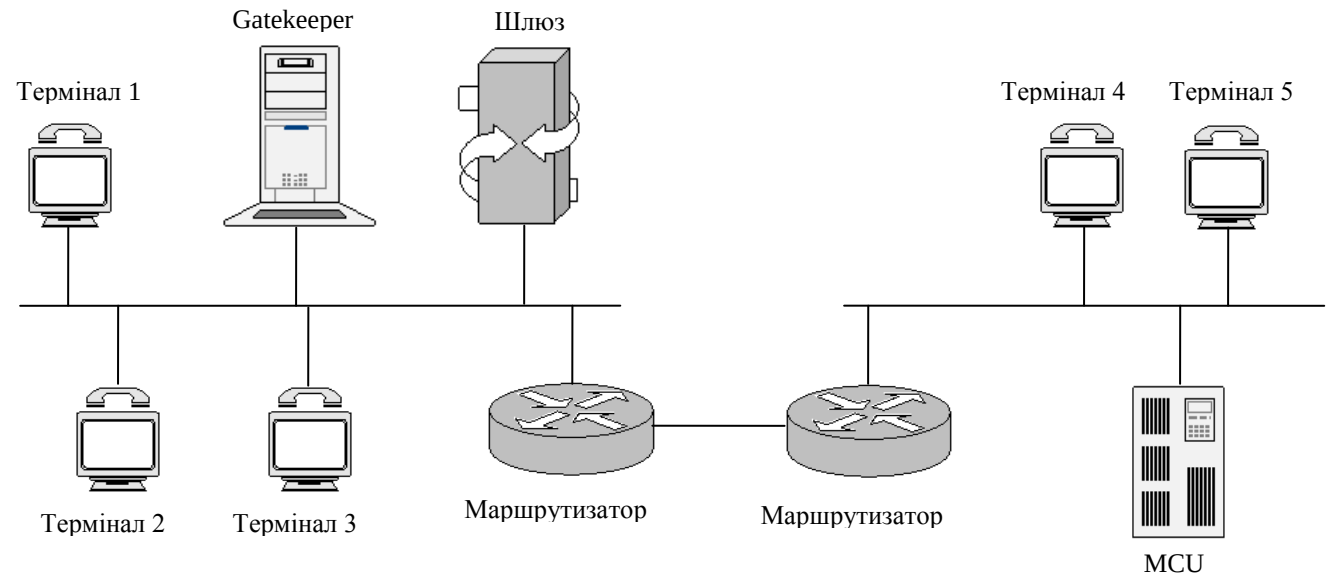


Рисунок 3.2 Зона мережі H.323.

В одній мережі IP-телефонії, що відповідає вимогам рекомендації ITU H.323, може знаходитися декілька gatekeeper, взаємодіючих один з одним по протоколу RAS.

Крім основних функцій, визначених рекомендацією H.323, gatekeeper може відповідати за аутентифікацію користувачів і нарахування плати за телефонні з'єднання.

Пристрій керування конференціями забезпечує можливість організації зв'язку між трьома чи більше учасниками. Рекомендація H.323 передбачає три види конференції: централізована (тобто керована MCU, з яким кожен учасник конференції з'єднується в режимі точка-точка), децентралізована (коли кожен учасник конференції з'єднується з іншими її учасниками в режимі точка-група точок) і змішана.

Перевагою централізованої конференції є порівняно просте термінальне устаткування, недоліком - велика вартість пристрою керування конференціями.

Для децентралізованої конференції потрібно більш складне термінальне устаткування і бажано, щоб у мережі IP підтримувалася передача пакетів IP в режимі багатоадресної розсилки. Якщо цей режим у мережі не підтримується, термінал повинний передавати мовну інформацію кожному з інших учасників конференції в режимі точка-точка.

Пристрій керування конференціями складається з одного обов'язкового елемента - контролера конференції, (Multipoint Control - MC), і крім того може містити в собі один чи більше процесорів для обробки користувацької інформації (Multipoint Processor - MP). Контролер може бути фізично сполучений з gatekeeper, шлюзом чи пристроєм керування конференціями.

Контролер конференцій використовується для організації конференції будь-якого типу. Він організовує обмін між учасниками конференції даними про режими, підтримувані їхніми терміналами, і вказує, у якому режимі учасники

конференції можуть передавати інформацію, причому в ході конференції цей режим може змінюватися, наприклад, при підключенні до неї нового учасника.

Так як контролерів у мережі може бути декілька, для кожної знову створюваної конференції повинна бути проведена спеціальна процедура виявлення того контролера, що буде керувати даною конференцією.

При організації централізованої конференції, крім контролера МС, повинний використовуватися процесор МР, що обробляє користувацьку інформацію. Процесор МР відповідає за переключення чи змішування мовних потоків, відеоінформації і даних. Для децентралізованої конференції процесор не потрібний.

Існує ще один елемент мережі Н.323 - *проксі-сервер Н.323,* тобто сервер-посередник. Цей сервер функціонує на прикладному рівні. Проксі-сервер може визначати, з яким додатком (Н.323 чи іншим) асоційований виклик, і здійснювати потрібне з'єднання. Проксі-сервер виконує наступні ключові функції:

• підключення через засоби доступу, що комутується, чи локальні мережі терміналів, що не підтримують протокол резервування ресурсів (RSVP). Два таких проксі-сервера можуть утворити в IP-мережі тунельне з'єднання з заданою якістю обслуговування;

• маршрутизацію трафіка Н.323 окремо від звичайного трафіка даних;

• забезпечення сумісності з перетворювачем мережевих адрес, оскільки допускається розміщення устаткування Н.323 у мережах із простором адрес приватних мереж;

• захист доступу - тільки для трафіка Н.323.

Протокол RAS (Registration, Admission, Status) забезпечує взаємодію кінцевих чи інших пристроїв з gatekeeper. Основними функціями протоколу є: реєстрація пристрою в системі, контроль його доступу до мережевих ресурсів, зміна смуги пропускання в процесі зв'язку, опитування та індикація поточного стану пристрою. Як транспортний протокол використовується протокол з негарантованою доставкою інформації UDP.

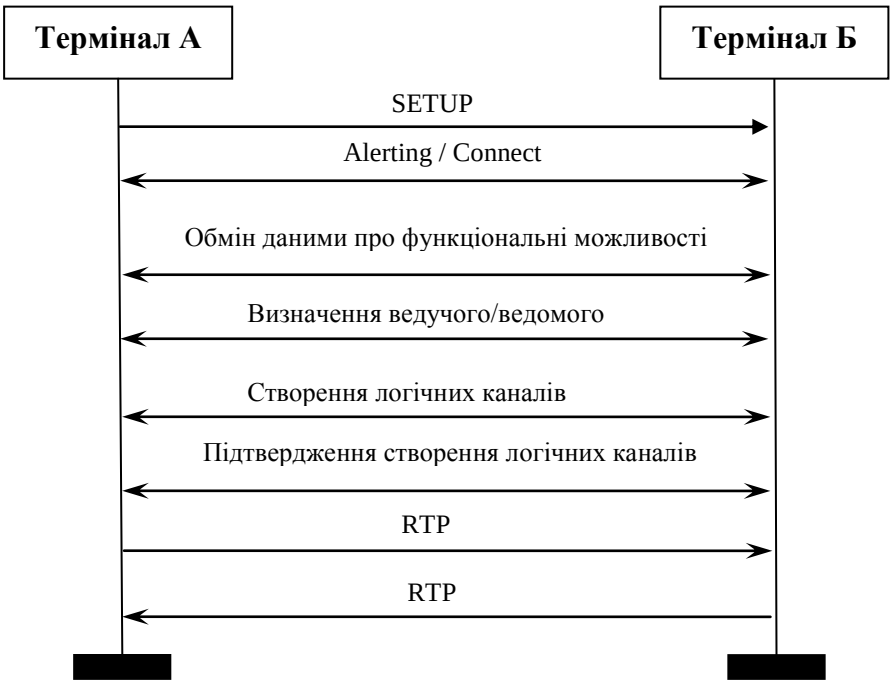
Протокол Н.225.0 (Q.931) підтримує процедури встановлення, підтримки і руйнування з'єднання. Як транспортний протокол використовується протокол із встановленням з'єднання і гарантованою доставкою інформації TCP.

По протоколі Н.245 відбувається обмін між учасниками з'єднання інформацією, що необхідна для створення логічних каналів. По цих каналах передається мовна інформація, упакована в пакети RTP/UDP/IP.

Виконання процедур, передбачених протоколом RAS, є початковою фазою встановлення з'єднання з використанням сигналізації Н.323. Далі випливають фаза сигналізації Н.225.0 (Q.931) і обмін керуючими повідомленнями Н.245. Руйнування з'єднання відбувається в зворотній послідовності; у першу чергу закривається керуючий канал Н.245 і сигнальний канал Н.225.0, після чого gatekeeper по каналі RAS повідомляється про звільнення раніше зайнятої смуги пропускання.

Спрощений сценарій з’єднання розглянутий на мал.3.3.

1. Кінцевий пристрій користувача А надсилає запит з'єднання - повідомлення SETUP - до кінцевого пристрою користувача Б на TCP-порт 1720.
2. Кінцевий пристрій викликуваного користувача Б відповідає на повідомлення SETUP повідомленням ALERTING, що означає: пристрій вільний, а викликуваному користувачу подається сигнал про вхідний виклик.
3. Після того, як користувач Б приймає виклик, стороні А передається повідомлення CONNECT з номером TCP-порта керуючого каналу H.245.
4. Кінцеві пристрої обмінюються по каналі H.245 інформацією про типи використовуваних мовних кодексі (G.729,G.723.1 іт.д.), а також про інші функціональні можливості устаткування, і оповіщають один одного про номери портів UDP на які потрібно передавати інформацію.
5. Відкриваються логічні канали для передачі мовної інформації.
6. Мовна інформація передається в обидва боки повідомленнями протоколу RTP; крім того, ведеться контроль передачі інформації за допомогою протоколу RTCP.



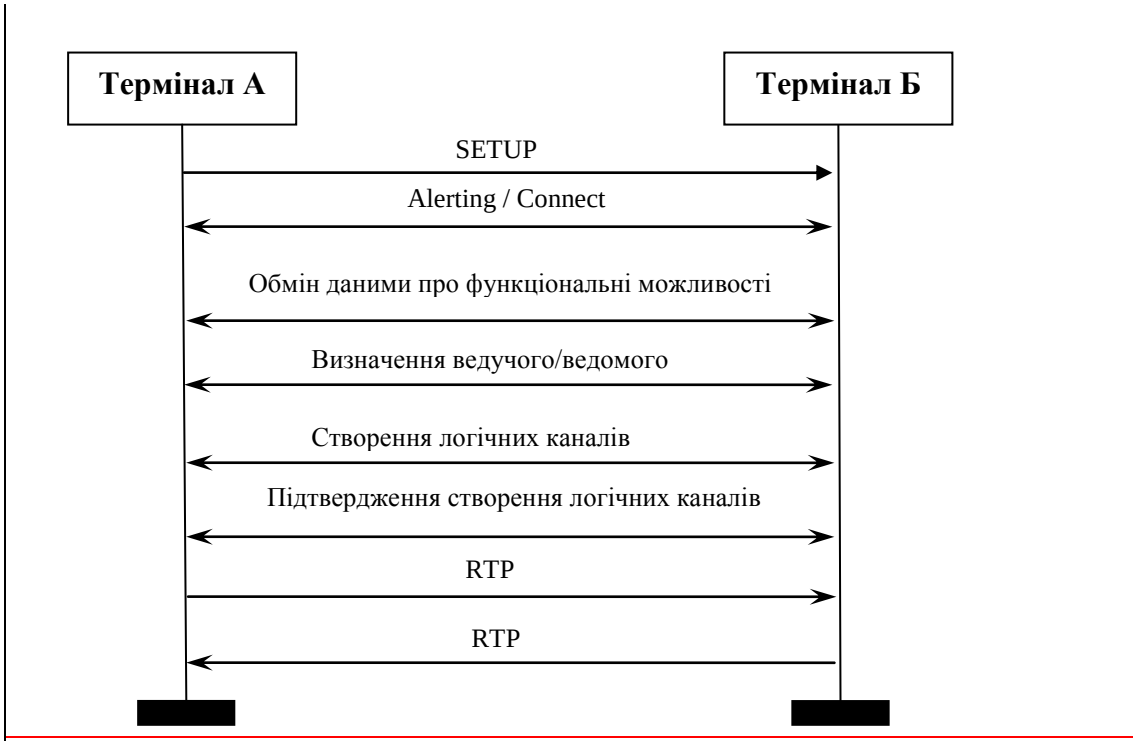


Рисунок 3.3 Спрощена схема встановлення з’єднання в мережі H.323.

Приведена процедура обслуговування виклику базується на протоколі H.323 версії 1. Версія 2 протоколу H.323 дозволяє передавати інформацію, необхідну для створення логічних каналів, безпосередньо в повідомленні SETUP протоколу H.225.0 без використання протоколу H.245. Така процедура називається “швидкий старт” і дозволяє скоротити кількість циклів обміну інформацією при встановленні з'єднання. Крім організації базового з'єднання, у мережах H.323 передбачене надання додаткових послуг відповідно до рекомендацій ITU.450.x.

3.2 Мережа на базі протоколу SIP.

Другий підхід до побудови мереж IP-телефонії, запропонований робочою групою MMUSIC комітету IETF у документі RFC 2543. SIP являє собою текст-орієнтований протокол, що є частиною глобальної архітектури мультимедіа, розробленої комітетом IETF. Ця архітектура також містить у собі протокол резервування ресурсів RSVP, транспортний протокол реального часу RTP, протокол передачі потоків у реальному часі RTSP, протокол опису параметрів зв'язку SDP, протокол повідомлення про зв'язок. Однак функції протоколу SIP не залежать від кожного з цих протоколів.

Відразу слід зазначити, що хоча на сьогодні найбільш широке поширення одержав протокол H.323, усе більша кількість виробників намагається передбачити у своїх нових продуктах підтримку протоколу SIP.

Підхід SIP до побудови мереж IP-телефонії простіший в реалізації, ніж протокол H.323, але менше підходить для організації взаємодії з телефонними мережами. В основному це зв'язано з тим, що протокол сигналізації SIP, базується на протоколі HTTP, який в свою чергу погано погоджується зі системами сигналізації, використовуваними в ТМЗК. Тому протокол SIP більш підходить

постачальникам послуг Інтернет для надання послуги IP-телефонії, причому ця послуга буде усього лише частиною пакета послуг.

Важливою особливістю протоколу SIP є підтримка мобільності користувача, тобто його здатності одержувати доступ до замовлених послуг у будь-якому місці і з будь-якого термінала, а також здатності мережі ідентифікувати й аутентифікувати користувача при його переміщенні з одного місця в інше. Ця властивість SIP не унікальна, і, наприклад, протокол H.323 теж у значній мірі підтримує таку можливість.

Не останню роль у підтримці мобільності користувача відіграє адресація, яка використовується протоколом SIP. Можна використовувати декілька типів адресів, це може бути як адреса подібна до адреси електронної пошти, так і адреса у форматі універсального вказівника ресурсів – URL (Universal Resource Locators), так звані SIP URL. Типи адрес, які можна використовувати у протоколі SIP приведені нище:

- ім’я@домен;
- ім’я@хост;
- ім’я@IP-адрес;
- №телефона@шлюз;

Таким чином SIP-адреса складається з двох частин: перша ідентифікує користувача, інша – станцію чи домен, де цей користувач зареєстрований. Четвертий формат SIP-адреси підходить для використання телефоном.

Приклади SIP-адрес приведені нище:

- sip:ost@imz.lviv.ua
- sip:user1@192.168.1.152
- sip:123-45-67@gateway.ua

На початку SIP-адреси стоїть слово “sip:”, яке вказує, що це саме SIP-адреса, так, наприклад як “http:” чи “mailto:”.

Архітектура протоколу SIP є подібною до архітектури протоколу HTTP, а отже це архітектура „клієнт-сервер”. Згідно цій архітектурі всі повідомлення поділяються на запроси клієнта до сервера та відповіді сервера клієнту. Структура повідомлень протоколу SIP представлена нижче.

Стартовий рядок
Заголовки
Пустий рядок
Тіло повідомлення

Рисунок 3.4 Структура повідомлень протоколу SIP

Стартовий рядок запиту містить в собі тип запиту, адресу призначення та номер версії протоколу. Якщо повідомлення є відповіддю на запит, то повідомлення містить тип відповіді, її коротка розшифровка та номер версії протоколу. Заголовок повідомлення містить інформацію необхідну для обслуговування даного повідомлення.

Для кращого розуміння того, що саме являє собою повідомлення SIP розглянемо типовий запит INVITE рис.3.5.

```
INVITE sip:ost@imz.lviv.ua SIP/2.0
        Via: SIP/2.0/UDP comp.lviv.ua
        From: Alf <sip: alf@imz.lviv.ua>
        To: OST <sip: ost@imz.lviv.ua>
        Call-ID: 2121546532@ comp.lviv.ua
        Cseq: 1 INVITE
        Content-Type: application/sdp
        Content-Length:...
        V=0
        O=alf 54988754 3265548798 IN IP4 128.192.21.54
        C=IN IP4 comp.lviv.ua
        m=audio 3456 RTP/AVP 0 3 4 5
```

Рисунок 3.5. Запит протоколу SIP.

В даному прикладі користувач Alf (alf@imz.lviv.ua) викликає користувача OST (ost@imz.lviv.ua). Заголовок Via служить для того, щоб уникнути ситуації, в якій запит може піти по замкнутому колу. Заголовки From і To призначені для ідентифікації відправника та адресата. Перед цими заголовками стоїть напис, який відправник бажає вивести на дисплей користувача, якого він викликає. Call-ID – особливий ідентифікатор сеансу зв'язку. Заголовок CSeq – особливий ідентифікатор запиту, який відноситься до одного з'єднання. Він служить для кореляції запиту з відповіддю на нього. Заголовок Content-Type визначає формат опису сеансу зв'язку. Content-Length – вказує на розмір тіла повідомлення. Останній рядок ідентифікує протокол та порт які відповідають за мовну інформацію. Цифри в кінці рядка означають який саме алгоритм кодування використовується.

Архітектура мережі, що базуються на протоколі SIP представлена на рис.3.6.

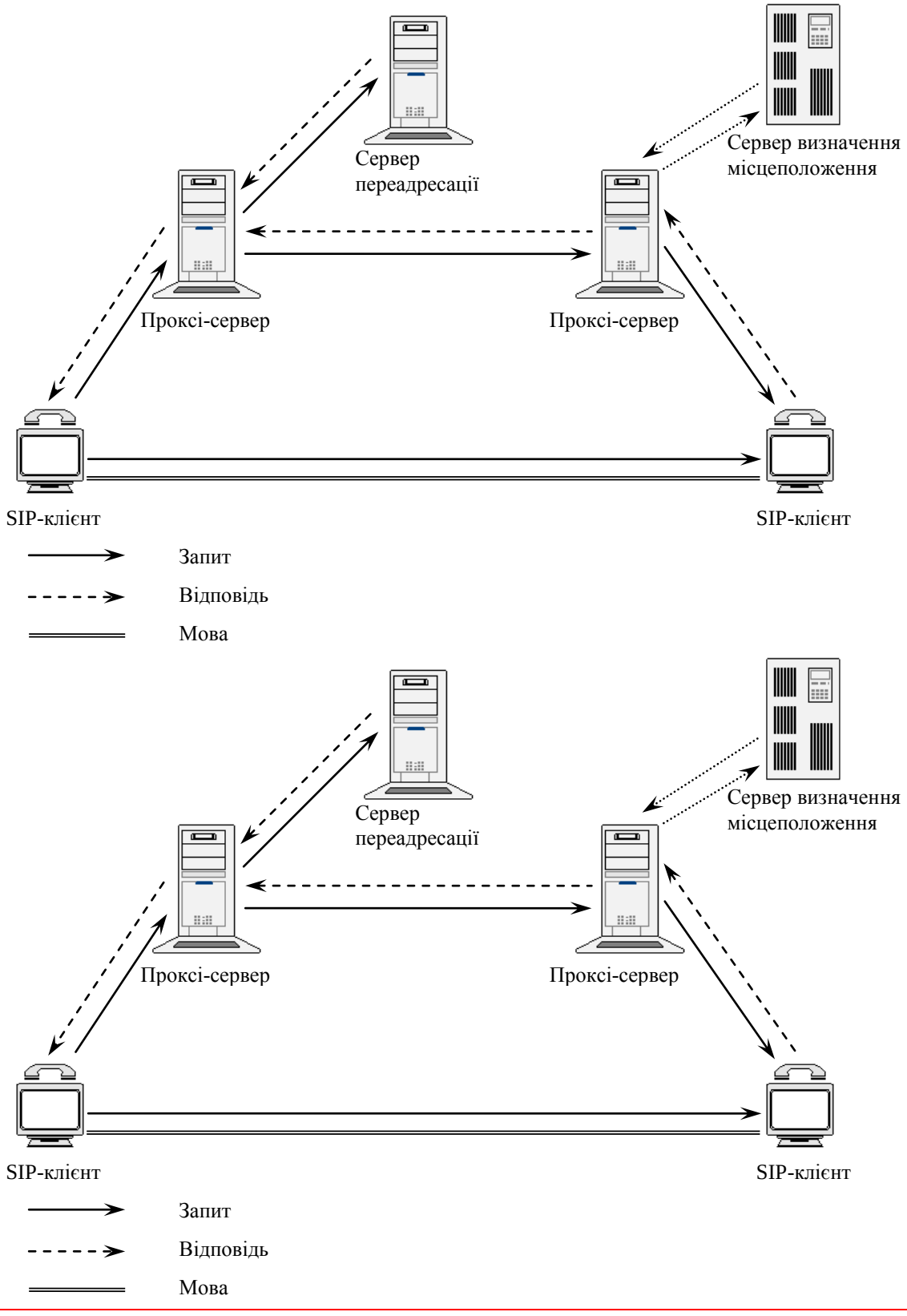


Рисунок 3.6 Архітектура мережі на базі протоколу SIP.

Мережа SIP містить три основні елементи: агент користувача, проксі-сервер і сервери переадресації.

Агент користувача є додатком термінального устаткування і містять у собі дві складові: агент користувача – клієнт (UAC) і агент користувача – сервер

(UAS), (*клієнт* та *сервер)*. Клієнт UAC ініціює SIP-запити. Сервер UAS приймає запити і повертає відповіді.

Проксі-сервер діє від імені інших клієнтів і містить функції клієнта і сервера. Цей сервер інтерпретує і може перезаписувати заголовки запитів перед відправленням їх до інших серверів.

Нижче представлений алгоритм установлення з'єднання за допомогою протоколу SIP при участі проксі-сервера рис.3.7:

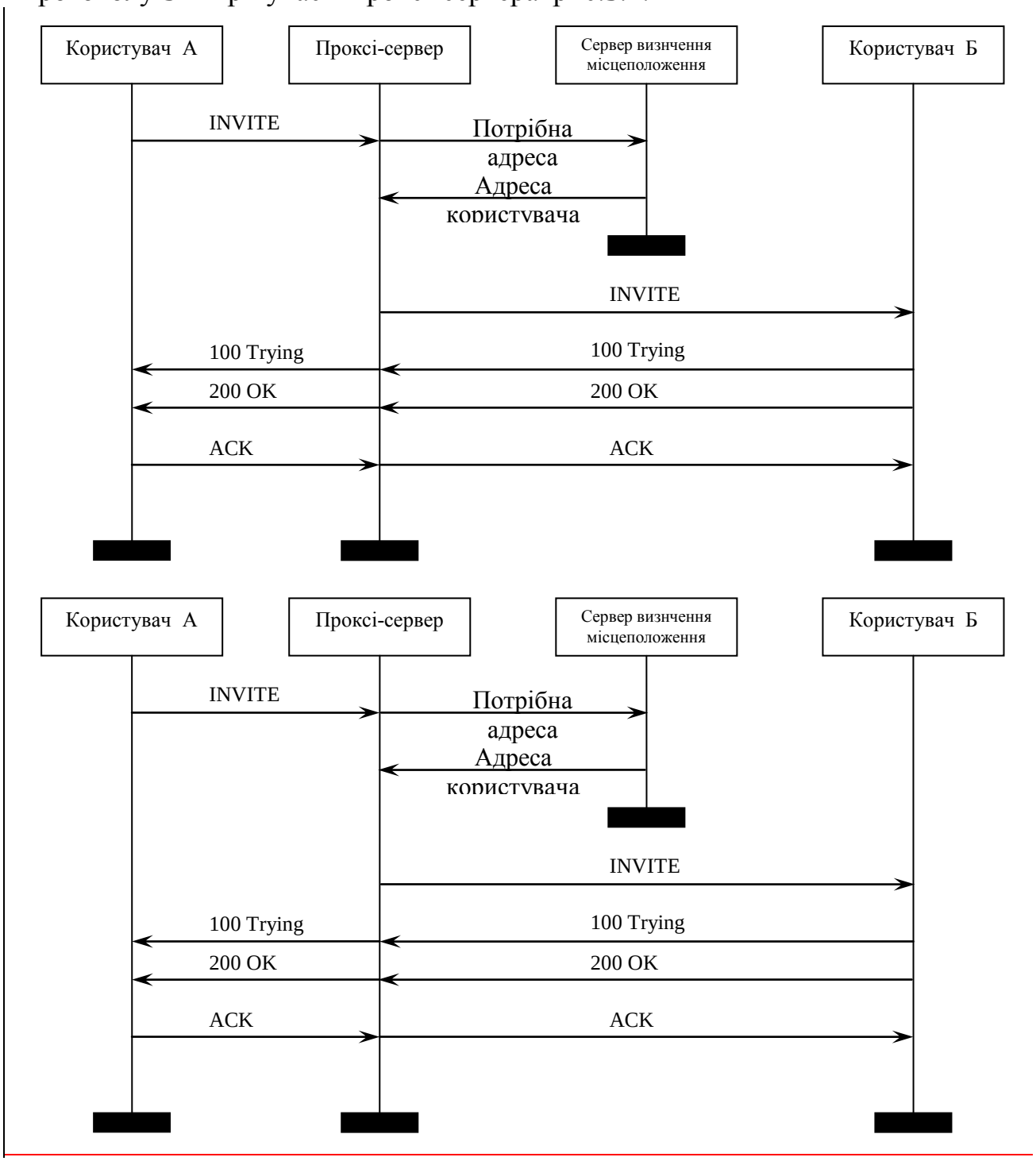


Рисунок 3.7 Встановлення з’єднання за участю проксі-сервера

1. Проксі-сервер приймає запит з'єднання INVITE від викличного устаткування користувача.

2. Проксі-сервер встановлює місцезнаходження клієнта за допомогою сервера визначення місця розташування .

3. Проксі-сервер передає запит INVITE викликуваному користувачу.

4. Устаткування викликуваного користувача повідомляє про вхідний виклик і повертає проксі-серверу повідомлення про те, що запит INVITE обробляється (код 100). Проксі-сервер, у свою чергу, направляє цю інформацію устаткуванню викличного користувача.

5. Коли викликуваний абонент приймає виклик, його устаткування сповіщає про це проксі-сервер (код 200), який, в свою чергу, перенаправляє інформацію про те, що виклик прийнятий, до устаткування викличного користувача.

6. Виклична сторона підтверджує встановлення з'єднання передачею запиту АСК. Встановлення з'єднання закінчене, абоненти можуть обмінюватися мовною інформацією.

Сервер переадресації визначає поточне місце розташування викликуваного абонента і повідомляє його викличному користувачу. Для визначення поточного місця розташування викликуваного абонента сервер переадресації звертається до *сервера визначення місця розташування.*

Алгоритм встановлення з'єднання з використанням протоколу SIP при участі сервера переадресації має наступний вигляд:

1. Сервер переадресації приймає від викличної сторони запит з'єднання INVITE і зв'язується із сервером визначення місцезнаходження, що видає поточну адресу потрібного користувача.

2. Сервер переадресації передає цю адресу викличній стороні. На відміну від проксі-сервера, запит INVITE до устаткування викликуваного користувача сервер переадресації не передає.

3. Устаткування викличного користувача підтверджує завершення транзакції із сервером переадресації запитом АСК.

4. Далі устаткування викличного користувача передає запит INVITE на адресу, отриману від сервера переадресації.

5. Устаткування викликуваного користувача повідомляє останнього про вхідний виклик і повертає викличному устаткуванню повідомлення про те, .що запит INVITE обробляється (код 100).

6. Коли викликуваний абонент приймає виклик, про це сповіщається устаткування викличного користувача (код 200). Встановлення з'єднання завершене, абоненти можуть обмінюватися мовною інформацією.

Протокол SIP передбачає 6 запитів і відповідей на них. Сигналізація SIP дає можливість користувацьким агентам і мережевим серверам визначати місце розташування, видавати запити і керувати з'єднаннями.

INVITE - запит залучає користувача чи послугу до участі у сеансі зв'язку і містить опис параметрів з’єднання. За допомогою цього запиту користувач може визначити функціональні можливості термінала свого партнера по зв'язку і

розпочати сеанс зв'язку використовуючи обмежене число повідомлень і підтверджень їхнього прийому.

АСК - запит підтверджує прийом відповіді на команду INVITE і завершує транзакцію.

OPTIONS - запит дозволяє одержати інформацію про функціональні можливості користувацьких агентів і мережевих серверів. Однак цей запит не використовується для організації сеансів зв'язку.

BYE - запит використовується сторонами для руйнування з'єднання. Перед тим, як зруйнувати з'єднання, користувацькі агенти відправляють цей запит до сервера, повідомляючи про намір припинити сеанс зв'язку.

CANCEL – запит дозволяє користувацьким агентам і мережевим серверам скасувати раніше переданий запит, якщо відповідь на нього ще не була отримана.

REGISTER - запит застосовується клієнтами для реєстрації інформації про місце розташування з використанням серверів SIP.

3.3. Мережа на базі протоколу MGCP .

Третій підхід до побудови мереж IP-телефонії, заснований на використанні протоколу MGCP, також запропонований комітетом IETF, робочою групою MEGACO.

При розробці цього протоколу робоча група MEGACO спиралася на мережеву архітектуру, що містить основні функціональні блоки трьох видів рис. 3.7:

• шлюз – Media Gateway (MG), що виконує функції перетворення мовної інформації, з боку ТМЗК з постійною швидкістю передачі, у вид, придатний для передачі по мережах з маршрутизацією пакетів IP (кодування й упакування мовної інформації в пакети RTP/UDP/IP, а також зворотне перетворення);

• контролер шлюзів – Call Agent, який виконує функції керування шлюзами;

• шлюз сигналізації – Signaling Gateway (SG), що забезпечує доставку сигнальної інформації, з боку ТМЗК, до контролера шлюзів і перенос сигнальної інформації в зворотному напрямку.

Таким чином, весь інтелект функціонально розподіленого шлюзу зосереджений в контролері, функції якого можуть бути розподілені між декількома комп'ютерними платформами. Шлюз сигналізації виконує функції STP - транзитного пункту мережі сигналізації ЗКС7. Самі шлюзи виконують тільки функції перетворення мовної інформації. Один контролер керує одночасно декількома шлюзами. В мережі можуть бути присутнім кілька контролерів. Передбачається, що вони синхронізовані між собою й узгоджено керують шлюзами. Разом з тим, MEGACO не визначає протоколу для синхронізації роботи контролерів. Повідомлення протоколу MGCP переносяться протоколом без гарантованої доставки повідомлень UDP.

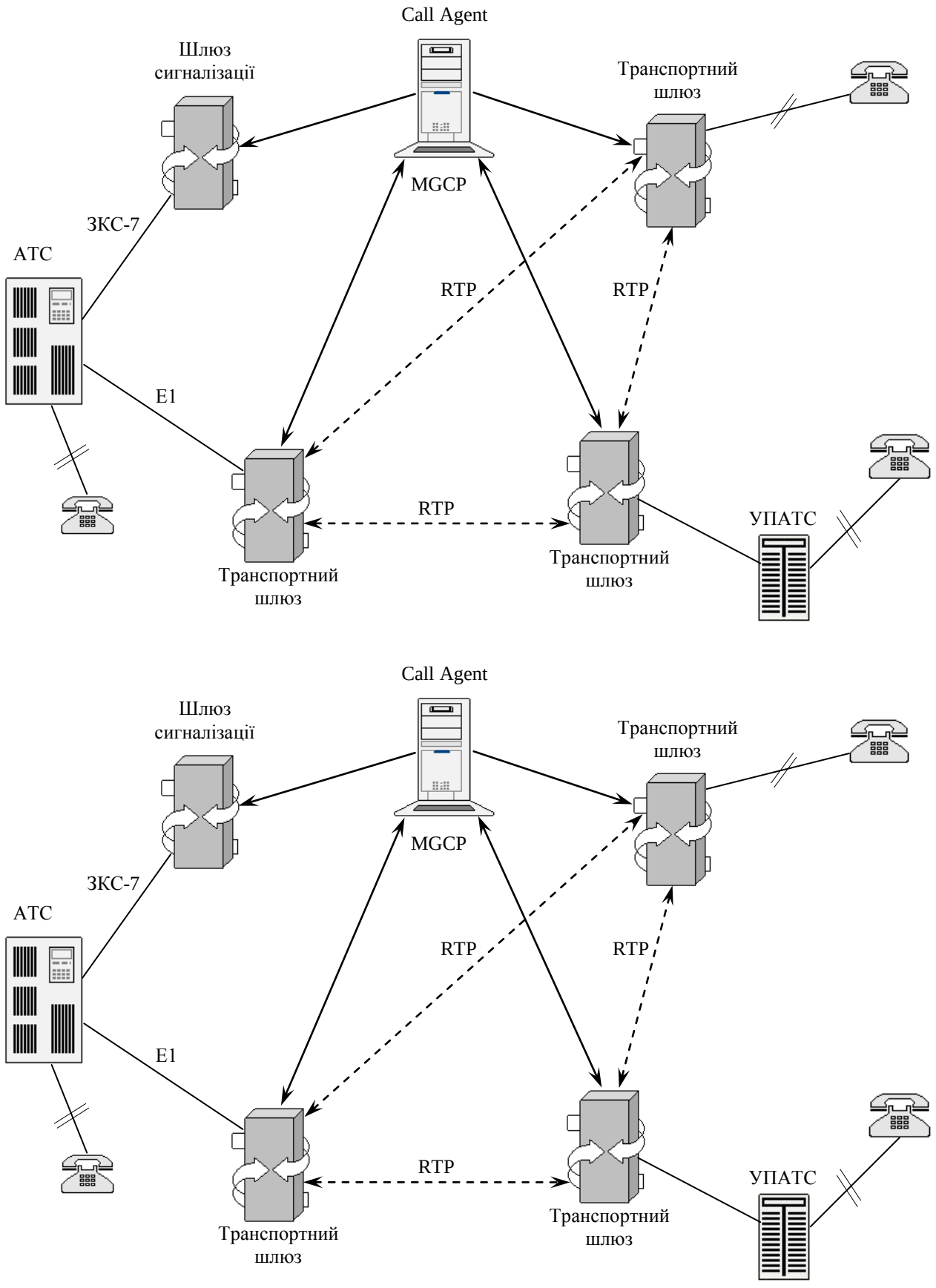


Рисунок 3.8 Архітектура мережі на базі протоколу MGCP.

Шлюз сигналізації приймає пакети трьох нижніх рівнів системи сигналізації ЗКС7 (рівнів підсистеми переносу повідомлень MTP) і передає сигнальні повідомлення верхнього, користувацького, рівня до контролера шлюзів. Шлюз сигналізації також повинен передавати по IP-мережі сигнальні повідомлення Q-931.

Відзначимо, що протокол MGCP є внутрішнім протоколом для обміну інформацією між функціональними блоками розподіленого шлюзу, що ззовні вбачається одним цілим. Контролер шлюзів є ведучим, а сам шлюз – керованим пристроєм, що повинен виконувати всі команди, що надходять від контролера Call Agent.

Вищеописані рішення забезпечують масштабованість мережі та простоту керування через контролер шлюзів. Шлюзи не є інтелектуальними пристроями, вимагають невисокої продуктивності процесорів і, отже, є більш дешевими.

Підхід, запропонований організацією IETF, добре підходить для розгортання глобальних мереж IP-телефонії, що приходять на зміну традиційним телефонним мережам.

малюнок 3.9 ілюструє взаємодію протоколу MGCP із протоколами ЗКС7 і H.323.

1. З телефонної станції АТС-А до шлюзу сигналізації SG1 по загальному каналі сигналізації надходить запит з'єднання (повідомлення IAM) На мал.3.8 шлюз сигналізації SG1 також сполучений із транспортним шлюзом TGW1. Шлюз SG1 передає повідомлення IAM контролеру шлюзів, що обробляє запит і визначає, що виклик повинен бути спрямований до кінцевого пристрою – терміналу H.323.

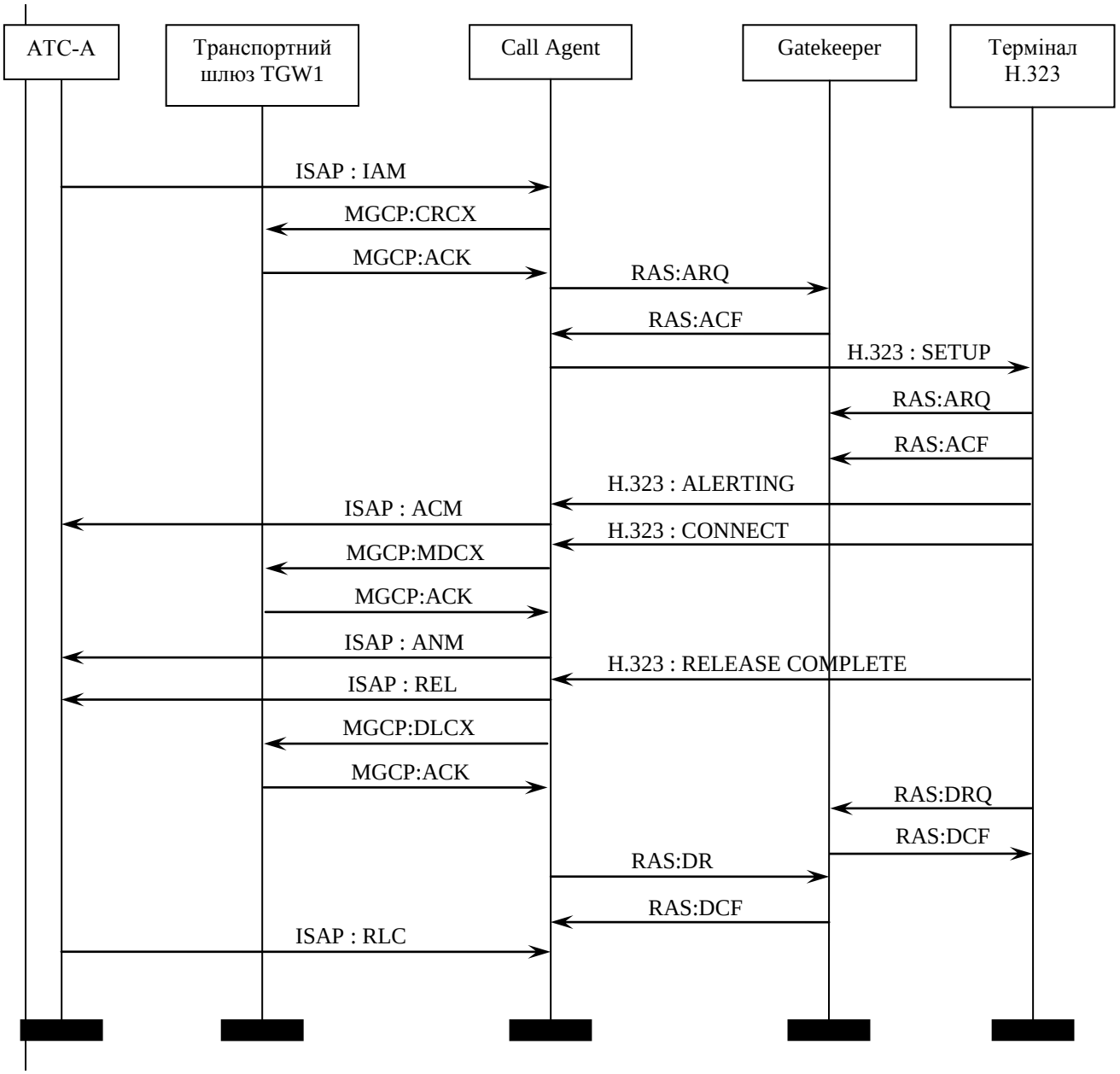
2. Контролер шлюзів резервує порт шлюзу TGW1 (розмовний канал). З цією метою він передає до шлюзу команду CreateConnection. І в цьому прикладі порт шлюзу TGW1 може тільки приймати інформацію (режим “recvonly”).

3. У відповіді на прийняту команду шлюз TGW1 повертає опис параметрів зв'язку.

4. Прийнявши відповідь від шлюзу TGW1, контролер передає до gatekeeper мережі H.323 повідомлення ARQ з alias адресою викликуваного абонента.

5. У відповідь на повідомлення ARQ gatekeeper передає повідомлення ACF із вказівкою транспортної адреси свого сигнального каналу.

6. Контролер передає запит з'єднання SETUP на транспортну адресу сигнального каналу gatekeeper, при цьому використовується процедура FastStart. Gatekeeper пересилає повідомлення SETUP до термінала, який викликається.


АТС-А
Транспортний шлюз TGW1
Call Agent
Gatekeeper
Термінал H.323
ISAP : IAM
MGCP:CRCX
MGCP:ACK
RAS:ARQ
RAS:ACF
H.323 : SETUP
RAS:ARQ
RAS:ACF
H.323 : ALERTING
ISAP : ACM
H.323 : CONNECT
MGCP:MDCX
MGCP:ACK
ISAP : ANM
H.323 : RELEASE COMPLETE
ISAP : REL
MGCP:DLCX
MGCP:ACK
RAS:DRQ
RAS:DCF
RAS:DR
RAS:DCF
ISAP : RLC

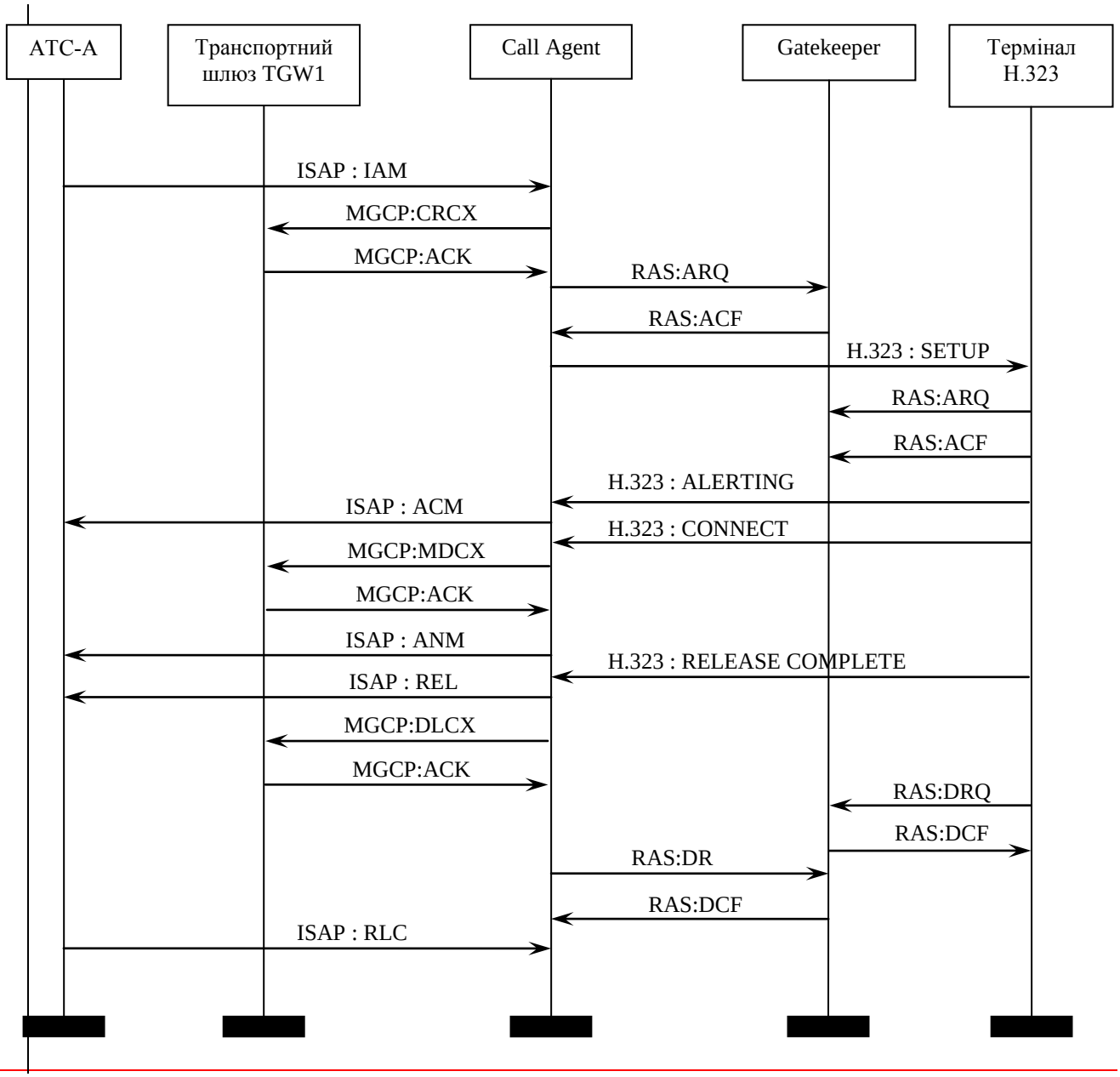


Рисунок 3.9 Встановлення та руйнування з’єднання з використанням протоколу MGCP.

7. Викликуваний термінал передає запит допуску до ресурсів мережі APQ.

8. У відповідь на запит APQ gatekeeper передає підтвердження запиту ACF.

9. Викликуваний термінал передає повідомлення ALERTING, яке gatekeeper маршрутизує до контролера шлюзів. При цьому викликуваному користувачу подається візуальний чи акустичний сигнал про вхідний виклик, а викличному користувачу подається індикація того, що викликуваний користувач не зайнятий і одержує сигнал про виклик.

10. Контролер перетворює повідомлення ALERTING у повідомлення ACM, що пересилається до АТС-А.

11. Після того як викликуваний користувач прийме вхідний виклик, контролер одержує повідомлення CONNECT.

12. Контролер шлюзів змінює в шлюзі TGW1 режим “recvonly” на повнодуплексний.

13. Шлюз TGW1 виконує і підтверджує зміну режиму з'єднання.

14. Контролер передає повідомлення ANM до АТС-А, після чого починається розмовна фаза з'єднання, в ході якої устаткування користувача, що викликав, передає мовну інформацію, упаковану в пакети RTP/UDP/IP, на транспортну адресу RTP-каналу термінала викликуваного абонента, а той, в свою чергу передає пакетовану мовну інформацію на транспортну адресу RTP-каналу термінала абонента, що викликав. За допомогою каналу RTCP ведеться контроль передачі інформації по RTP каналу.

15. Після закінчення розмовної фази починається фаза руйнування з'єднання. Устаткування користувача, що ініціює руйнування з'єднання, повинне припинити передачу мовної інформації, закрити логічні канали і передати повідомлення RELEASE COMPLETE, після чого сигнальний канал закривається.

16. Контролер шлюзів передає дане повідомлення до АТС-А з метою завершення з'єднання.

17. Крім того, контролер передає до шлюзу команду DLCX.

18. Шлюз підтверджує завершення з'єднання і передає до контролера зібрані за час з'єднання статистичні дані.

19. Після вищеописаних дій контролер і кінцеве устаткування сповіщають gatekeeper про звільнення смуги пропускання. З цією метою кожен з учасників з'єднання посилає gatekeeper по каналі RAS запит виходу зі з'єднання DRQ, на який gatekeeper повинен передати підтвердження DCF.

20. Від АТС-А приходить підтвердження роз'єднання RLC, після чого з'єднання вважається зруйнованим.

Варто помітити, що алгоритм взаємодії протоколів SIP та MGCP не сильно відрізняється від вищеописаного алгоритму.

4.ПРОТОКОЛ УПРАВЛІННЯ ШЛЮЗАМИ В МЕРЕЖАХ MGCP

4.1 Принцип декомпозиції шлюзу

У недавньому минулому робоча група MEGACO комітету IETF розробила протокол управління шлюзами - Media Gateway Control Protocol (MGCP). При розробці протоколу управління шлюзами робоча група MEGACO спиралася на принцип декомпозиції, згідно якому шлюз розбивається на окремі функціональні блоки (рис. 4.1):

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

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

• шлюз сигналізації - Signaling Gateway, який забезпечує доставку сигнальної інформації, що поступає з боку ТФОП, до пристрою управління шлюзом і перенесення сигнальної інформації у зворотному напрямі.

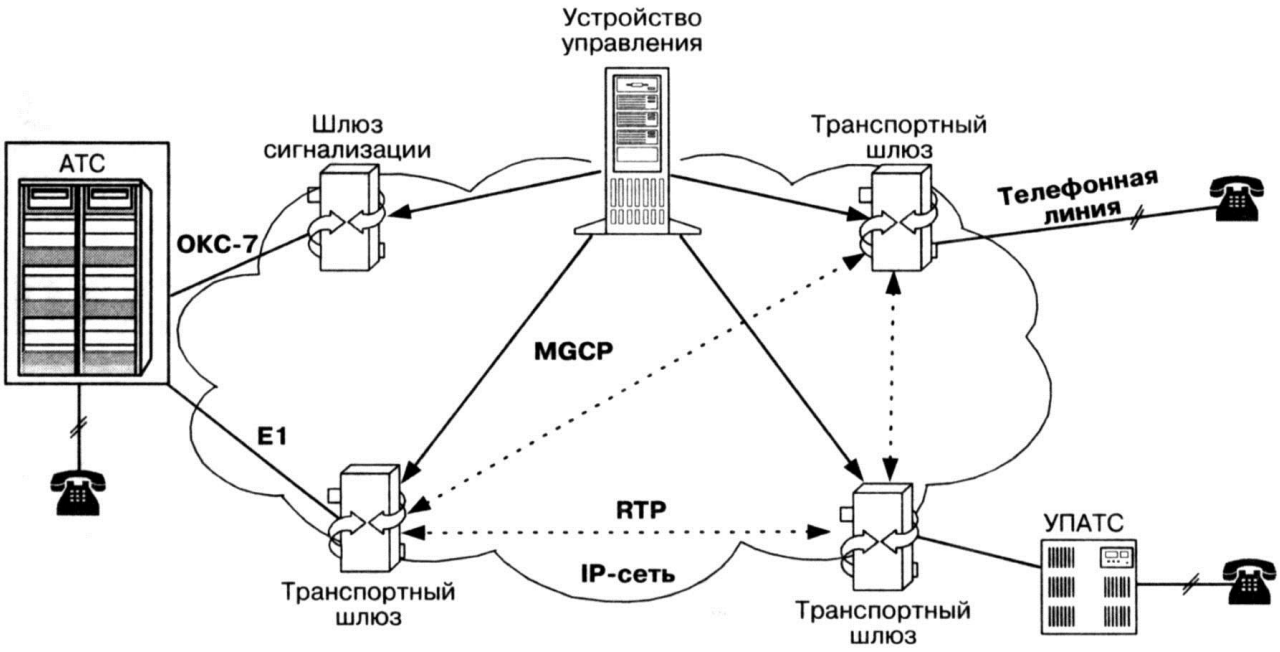


Рисунок 4.1 Архітектура мережі, що базується на протоколі MGCP

Таким чином, весь інтелект функціонально розподіленого шлюзу розміщується в пристрої управління, функції якого, у свою чергу, можуть бути розподілені між декількома комп'ютерними платформами. Шлюз сигналізації виконує функції STP - транзитного пункту системи сигналізації по загальному каналу - ОКС7. Транспортні шлюзи виконують тільки функції перетворення мовної інформації. Один пристрій управління обслуговує одночасно декілька шлюзів. У мережі може бути присутньо декількох пристроїв управління. Передбачається, що ці пристрої синхронізовани між собою і погоджено управляють шлюзами, що беруть участь в з'єднанні. Робоча група MEGACO не визначає протокол синхронізації роботи пристроїв управління, проте у ряді робіт, присвячених дослідженню можливостей

протоколу MGCP, для цієї мети пропонується використовувати протоколи H.323, SIP або ISUP/IP (рис. 4.2).

Перенесення повідомлень протоколу MGCP забезпечує протокол не гарантованої доставки - UDP. Крім того, робоча група SIGTRAN комітету IETF в даний час розробляє механізм взаємодії пристрою управління і шлюзу сигналізації. Останній повинен приймати поступаючі з ТФОП сигнальні одиниці підсистеми MTP системи сигналізації ОКС7 і передавати сигнальні повідомлення верхнього, призначеного для користувача рівня до пристрою управління. Основна увага робочої групи SIGTRAN приділена питанням розробки найбільш ефективного механізму передачі сигнальної інформації по IP-мережах. Слід зазначити, що існує декілька причин, вже згадуваних раніше, по яких довелося відмовитися від використання для цієї мети протоколу TCP. Замість нього робоча група SIGTRAN пропонує використовувати протокол Stream Control Transport Protocol (SCTP), який має ряд переваг перед протоколом TCP. Основною з цих переваг є значне зниження часу доставки сигнальної інформації і, отже, часу встановлення з'єднання - одного з найважливіших параметрів якості обслуговування.

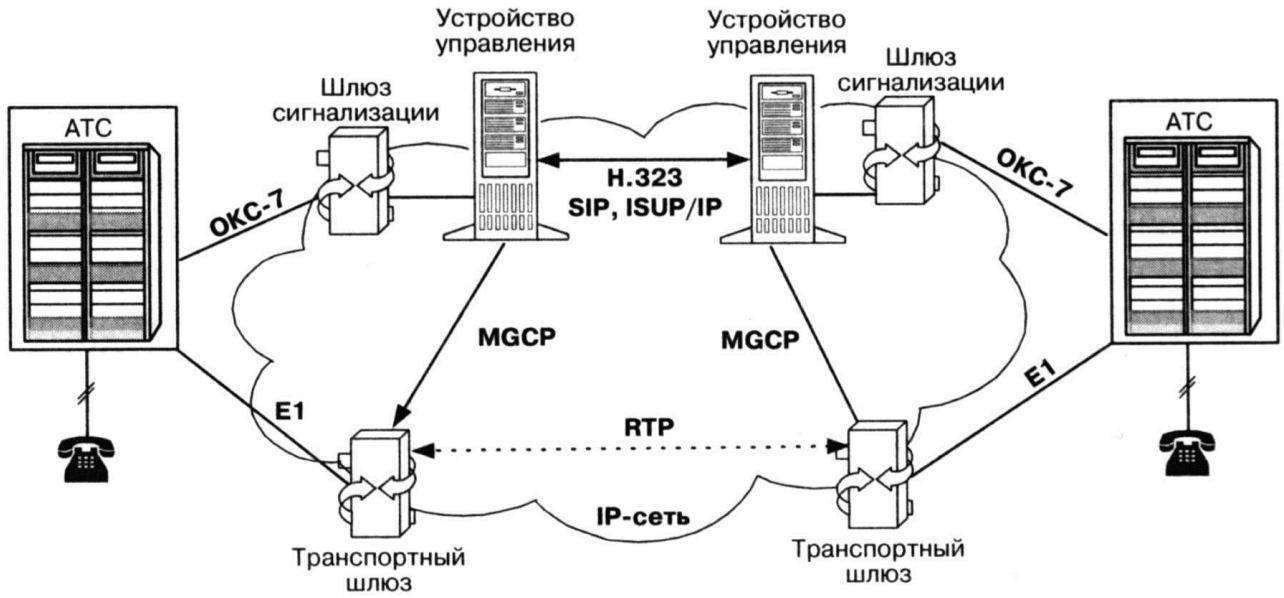


Рисунок 4.2 Синхронізація роботи пристроїв управління

Якщо розподілений шлюз підключається до ТФОП за допомогою сигналізації по виділених сигнальних каналах (ВСК), то сигнальна інформація разом з призначеною для користувача інформацією спочатку поступає в транспортний шлюз, а потім передається в пристрій управління без посередництва шлюзу сигналізації.

Одна з основних вимог, що пред'являються до протоколу MGCP, полягає в тому, що пристрої, які реалізовують цей протокол, повинні працювати в режимі без збереження інформації про послідовність транзакцій між пристроєм управління і транспортним шлюзом, тобто в пристроях не вимагається реалізації кінцевого автомата для опису цієї послідовності. Проте не слід поширювати подібний підхід

на послідовність станів з'єднань, відомості про яких зберігаються в пристрої управління.

Відзначимо, що протокол MGCP є внутрішнім протоколом, що підтримує обмін інформацією між функціональними блоками розподіленого шлюзу. Протокол MGCP використовує принцип master/slave (провідний/відомий), причому пристрій управління шлюзами є ведучим, а транспортний шлюз - відомим пристроєм, що виконує команди, що поступають від пристрою управління.

Таке рішення забезпечує масштабованість мережі і простоту експлуатаційного управління нею через пристрій управління шлюзами. До того ж, не інтелектуальні шлюзи вимагають меншої продуктивності процесорів і, як наслідок, виявляються менш дорогими. Крім того, забезпечується можливість швидко додавати нові протоколи сигналізації і нові додаткові послуги, оскільки потрібні для цієї зміни зачіпають тільки пристрій управління шлюзами, а не самі шлюзи.

Основний недолік цього підходу - незавершеність стандартів. Функціональні блоки розподілених шлюзів, розроблені різними фірмами-виробниками телекомунікаційного устаткування, практично несумісні. Функції пристрою управління шлюзами точно не визначені. Не стандартизовані механізми перенесення сигнальної інформації від шлюзу сигналізації (Signalling Gateway) до пристрою управління і у зворотному напрямі. До недоліків можна віднести також відсутність стандартизованого протоколу взаємодії між пристроями управління. Крім того, протокол MGCP, будучи протоколом управління шлюзами, не призначений для управління з'єднаннями за участю термінального устаткування користувачів (IP-телефонами). Це означає, що в мережі, побудованій на базі протоколу MGCP, для управління терміналами повинні бути присутніми сторож або сервер SIP (рис. 4.3).

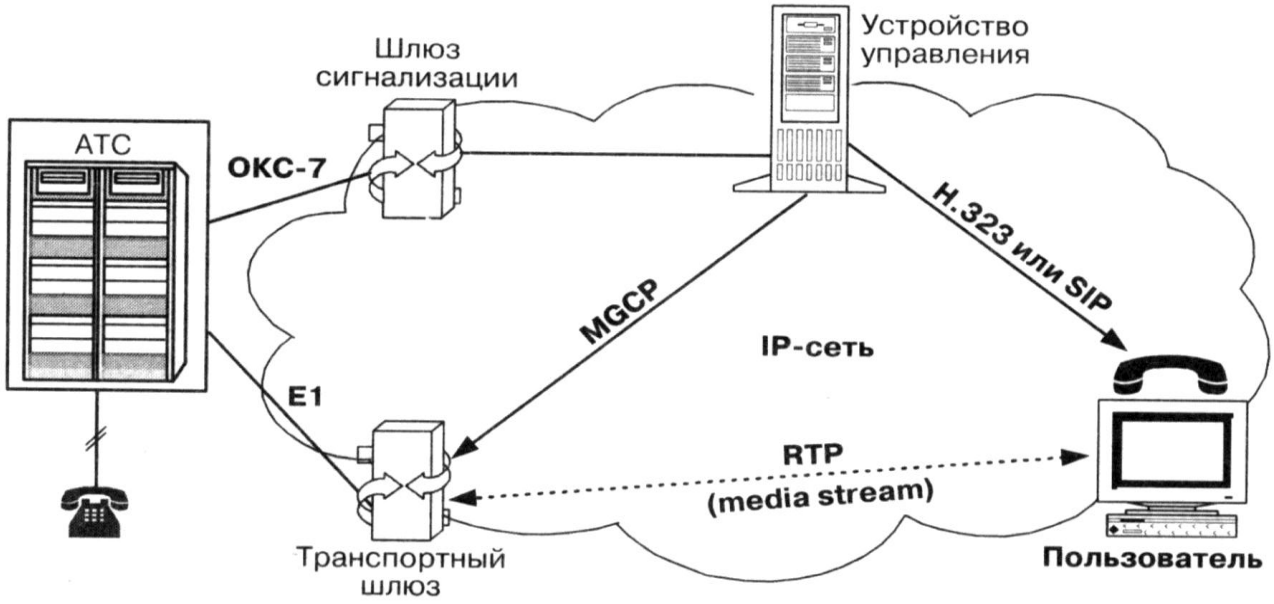


Рисунок 4.3 Управління терміналами в мережі, що базується на протоколі MGCP

4.2 Класифікація шлюзів

Робочою групою MEGACO запропонована наступна класифікація транспортних шлюзів (Media Gateways):

• Trunking Gateway - шлюз між ТФОП і мережею з маршрутизацією пакетів IP, орієнтований на підключення до телефонної мережі за допомогою великої кількості цифрових трактів (від 10 до декількох тисяч) з використанням системи сигналізації ОКС 7;

• Voice over ATM Gateway - шлюз між ТФОП і АТМ-СЕТЬЮ, який також підключається до телефонної мережі за допомогою великої кількості цифрових трактів (від 10 до декількох тисяч);

• Residential Gateway - шлюз, що підключає до IP-мережі аналогові, кабельні модеми, лінії xDSL і широкосмугові пристрої бездротового доступу;

• Access Gateway - шлюз для підключення до мережі IP-телефонії невеликої учрежденческой АТС через аналоговий або цифровий інтерфейс;

• Business Gateway - шлюз з цифровим інтерфейсом для підключення до мережі з маршрутизацією IP-пакетів учрежденческой АТС при використанні, наприклад, системи сигналізації DSS1;

• Network Access Server - сервер доступу до IP-мережі для передачі даних;

• Circuit switch або packet switch - комутаційні пристрої з інтерфейсом для управління від зовнішнього пристрою.

4.3 Модель організації зв'язку

Для опису процесу обслуговування виклику з використанням протоколу MGCP робочою групою MEGACO розроблена модель організації з'єднання - Connection model. Базою моделі є компоненти двох основних видів: порти (Endpoints) і підключення (Connections).

Endpoints - це порти устаткування, що є джерелами і приймачами інформації. Існують порти двох видів: фізичні і віртуальні. Фізичні порти - це аналогові інтерфейси, що підтримують кожен одне телефонне з'єднання, або цифрові канали, що також підтримують одне телефонне з'єднання і мультіплексування за принципом тимчасового розділення каналів в тракт Е1. Прикладом віртуального порту є джерело мовної інформації в інтерактивному мовному сервері, тобто якийсь програмний засіб.

Connection - означає підключення порту до одного з двох кінців з'єднання, яке створюється між ним і іншим портом. Таке з'єднання буде встановлено після підключення іншого порту до його другого кінця. З'єднання може зв'язувати порти різних шлюзів через мережу з маршрутизацією пакетів IP або порти усередині одного шлюзу.

На рисунку 4.4 представлені приклади використання цих двох компонентів. Відзначимо, що порти деяких видів можуть брати участь в декількох з'єднаннях одночасно.

Підключення до N з'єднань

а) цифровий порт

Підключення до M з'єднанням

б) аналоговий порт

Підключення до одного з'єднання
в) порт, що передає мовні сповіщення
Підключення до одного з'єднання
г) інтерактивна мовна система
Підключення до L з'єднань
д) порт, що підтримує конференцсвязь
Підключення до 2 з'єднань
е) міжмережевий екран або транскодер - порт ретрансляції пакетів
Підключення до одного з'єднання
ж) порт запису/відтворення телефонних розмов
Підключення до До з'єднань
з) АТМ-ІНТЕРФЕЙС

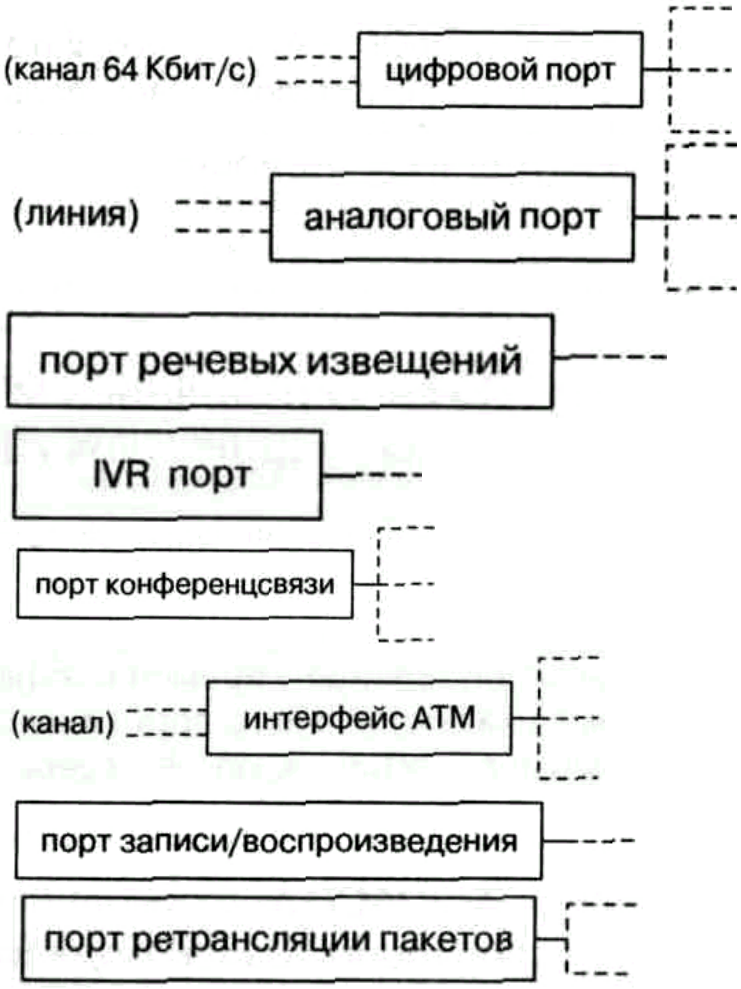


Рисунок 4.4 Приклади використання компонентів моделі

Підключення створюються пристроєм управління Call Agent для кожного порту, що бере участь в з'єднанні. На рисунку 4.5 показана ситуація, коли один пристрій управління контролює роботу двох портів різних шлюзів при організації з'єднання між цими портами.

4.4 Команди протоколу MGCP

В ході встановлення, підтримки і руйнування з'єднання за допомогою протоколу MGCP пристрій управління і шлюз обмінюються командами і відповідями, які є набором текстових рядків. У цьому параграфі дається короткий опис команд протоколу MGCP, серед яких визначені команди управління з'єднанням і команди управління портами устаткування.

За допомогою команди EndpointConfiguration пристрій управління інструктує шлюз, яким чином він повинен обробляти одержувані мовні сигнали, наприклад, використовувати для перетворення цифрового сигналу в аналогову форму закон А або закон |М.

Команда **EndpointConfiguration** містить ряд параметрів:

ReturnCode

<- EndpointConfiguration(Endpointid

Bearer Information),

де Endpointid - ідентифікатор порту шлюзу, до якого відноситься дана команда;

Bearerlnformation - параметр, що визначає закон (А або |і) декодування прийнятої мовної інформації.

ReturnCode - параметр, що повертається шлюзом пристрою управління, щоб інформувати його про виконання команди. Даний параметр є цілим числом, за яким можуть слідувати коментарі.

Call Agent за допомогою команди **Notification Request** може дати вказівку шлюзу виявляти певні події або сигнали і інформувати про них пристрій управління. До числа подій (сигналів), що детектують, входить зміна опору абонентського шлейфу, що відбувається, коли абонент піднімає або кладе трубку, а також отримання сигналів апаратів, факсиміле, і сигналів DTMF.

Команда NotificationRequest включає наступні параметри (у квадратних дужках вказані ті з них, які не є обов'язковими).

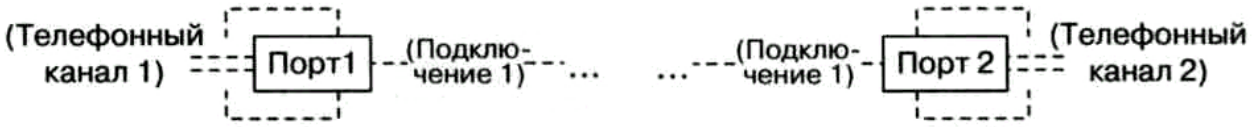


Рисунок 4.5 З'єднання в мережі, побудованій на базі

ReturnCode

<—NotificationRequest(Endpointid,

[NotifiedEntity,] [RequestedEvents,] Requestldentifier, [DigitMap,] [SignalRequests,] [QuarantineHandling,] [DetectEvents,] [encapsulated EndpointConfiguration])

Тут NotifiedEntity - ідентифікатор пристрою, якому повинна бути передана відповідь на команду. За відсутності цього параметра відповідь передається тому пристрою, від якого одержаний запит Notification Request.

Requested Events - список подій, про які слід оповістити пристрій, що управляє. Крім того, в цьому параметрі може бути вказано, як шлюз повинен реагувати на подію. Визначені наступні дії шлюзу: оповістити Call Agent про подію негайно; чекати подальших подій; якщо подія полягає в отриманні сигналу DTMF, то

накопичувати такі сигнали відповідно до вимог параметра DigitMap; у певних ситуаціях передавати в телефонний канал акустичні або зухвалі сигнали;

обробити інкапсульовану команду EndpointConfiguration; ігнорувати подію і т.д.

RequestIdentifier - ідентифікатор запиту, у відповідь на який передається команда.

DigitMap - необов'язковий параметр, що специфікує правила обробки сигналів DTMF. У цьому параметрі указує кількість сигналів, які шлюз повинен накопичити для передачі їх пристрою управління.

SignalRequests - сигнали, які повинні бути передані в канал, наприклад, сигнал посилки виклику.

QuarantineHandling - необов'язковий параметр, що визначає правила обробки подій, які були виявлені до моменту отримання даної команди в період так званого карантину (quarantine period) і про які Call Agent ще не був оповіщений.

DetectEvents - необов'язковий параметр, що визначає події, які потрібно виявити в період карантину, але не оповіщати про них Call Agent до отримання наступної команди NotificationRequest з включеним в неї параметром QuarantineHandling.

Encapsulated EndpointConfiguration - команда EndpointConfiguration, інкапсульована в команду NotificationRequest.

Решта параметрів команди тотожна описаним вище.

За допомогою команди **Notify** шлюз інформує пристрій управління про те, що відбулося подія з числа вказаних в команді NotificationRequest. Команда Notify містить наступні параметри:

ReturnCode
<- Notify (Endpointid
[NotifiedEntity] RequestIdentifier, ObservedEvents)

Тут ObservedEvents - параметр, в якому описуються події, що відбулися, наприклад, передаються набрані цифри номера. Решта параметрів була описана раніше.

За допомогою команди **CreateConnection** пристрій, що управляє, може дати шлюзу вказівку створити з'єднання двох портів одного і того ж шлюзу або різних шлюзів.

Структура цієї команди приведена нижче.

ReturnCode, Connectionid [SpecificEndPolntId,1 [LocalConnectionDescriptor] [SecondEndPointId] [SecondConnectionId] <- CreateConnection(Calllld
Endpointid
[NotifiedEntity]
[LocalConnectionOptions]
Mode
[{RemoteConnectionDescriptor I
SecondEndpointId),]
[Encapsulated NotificationRequest] про [Encapsulated EndpointConfiguration])

Calllld - унікальний параметр, що ідентифікує сесію, до якої відноситься дане з'єднання.

NotifiedEntity - необов'язковий параметр, що ідентифікує пристрій, до якого повинні бути передані команди Notify або DeleteConnection.

LocalConnectionOptions - параметр, використовуваний Call Agent, щоб дати шлюзу вказівки відносно характеристик підключення порту до з'єднання. У параметр можуть входити наступні поля:

метод кодування, розмір мовних пакетів, смуга пропускання, тип обслуговування, використання ехокомпенсатора, використання режиму придушення пауз в розмові, використання режиму придушення шуму, використання резервування ресурсів і інші поля. Кодування трьох перших полів повинне проводитися відповідно до протоколу опису сесій SDP (Session Description Protocol), причому Call Agent може у казать тільки смугу пропускання і залишити за шлюзом право вибору методу кодування і розмірів мовних пакетів.

Mode - параметр, що визначає режим роботи для даного кінця з'єднання. Визначені наступні режими: передача, прийом, прийом/передача, конференція, дані, відсутність активності, петля, тестовий режим та інші.

RemoteConnectionDescriptor - опис підключення до з'єднання на другом його кінці. Даний параметр містить ті ж поля, що і параметр LocalConnectionOptions. Ці поля також повинні кодуватися відповідно до протоколу SDP. Варто відзначити, що при створенні з'єднання між двома шлюзами, при передачі першої команди CreateConnection параметр RemoteConnectionDescriptor відсутній (йому привласнюється нульове значення), оскільки інформація про підключення до з'єднання на другом його кінці у цей момент відсутній. Не маючи такої інформації, тобто не одержавши команду ModifyConnection, шлюз може тільки приймати інформацію (працювати в режимі receive only).

SecondEndpointId - цей параметр може включатися в команду CreateConnection замість параметра RemoteConnectionDescriptor при встановленні з'єднання між двома портами одного і того ж шлюзу.

Encapsulated NotificationRequest - інкапсульована команда NotificationRequest.

У відповідь на команду CreateConnection, окрім описаного вище параметра ReturnCode, шлюз повертає наступні параметри:

Connectionid - унікальний ідентифікатор підключення даного порту до з'єднання.

SpecificEndPointId - необов'язковий параметр, що ідентифікує порт, який відповідає на команду CreateConnection, якщо він не був специфікований пристроєм управління.

LocalConnectionDescriptor - параметр, що містить інформацію про IP-адресу і номер порту RTP відповідно до протоколу SDP.

SecondEndPointId - параметр, що означає, що команда CreateConnection створила два з'єднання.

SecondConnectionId - ідентифікатор підключення для другого з'єднання.

Пристрій управління може змінити параметри існуючого з'єднання за допомогою команди **ModifyConnection**, яка включає наступні параметри.

ReturnCode

[LocalConnectionDescriptor]

<--- ModifyConnection (Call Id

Endpointid, Connectionid [NotifiedEntity] [LocalConnectionOptions] [Mode]

[RemoteConnectionDescriptor] [Encapsulated NotificationRequest] [Encapsulated EndpointConfiguration])

Тут використовуються такі ж параметри, як і в команді CreateConnection, але додається обов'язковий параметр Connectionid, який ідентифікує підключення до з'єднання даного порту устаткування, оскільки один порт може одночасно мати підключення до декількох з'єднань.

Дана команда може використовуватися для передачі інформації про інший кінець з'єднання в параметрі RemoteConnection Descriptor, для активизации/деактивизации з'єднання за допомогою параметра Mode, для зміни алгоритму кодування, періоду пакетізациі передаваної інформації або для управління придушенням луни.

Таким чином, якщо спочатку порт міг тільки приймати інформацію, оскільки не мав опису функціональних можливостей і адреси порту на іншому кінці з'єднання, то описувана команда створює можливість передавати інформацію.

Якщо параметри з'єднання на ближньому кінці були змінені, наприклад, був змінений номер порту RTP, то відповідає на команду ModifyConnection може повертатися параметр LocalConnection-Descriptor.

Пристрій управління може зруйнувати існуюче з'єднання за допомогою команди DeleteConnection. Крім того, за допомогою цієї команди шлюз може передати до Call Agent індикацію того, що існуюче з'єднання більше підтримуватися не може.

Команда **DeleteConnection**, що передається пристроєм управління, має наступний вигляд:

ReturnCode
Connection-parameters
<- DeleteConnection (Calllld/
Endpointid
Connectionid
[Encapsulated NotificationRequest]
[Encapsulated EndpointConfiguration])

Всі параметри були описані раніше, проте слід зазначити, що в параметр NotificationRequest може включатися інструкція, наприклад, про дії шлюзу при детектуванні розмикання абонентського шлейфу (абонент поклав трубку): в цьому випадку шлюз повинен зруйнувати з'єднання і чекати замикання шлейфу (наступного виклику).

У загальному випадку, команда DeleteConnection передається обом шлюзам, підключеним до з'єднання. Після завершення з'єднання у відповідь на команду DeleteConnection шлюз повертає статистичні дані, зібрані за час з'єднання - connection-parameters:

• кількість переданих RTP-пакетів
• кількість переданих байтів інформації, не рахуючи службової інформації (заголовків IP/UDP/RTP)
• кількість одержаних RTP-пакетів
• кількість прийнятих байтів інформації, не рахуючи службової інформації (заголовків IP/UDP/RTP)

• кількість втрачених RTP-пакетів
• варіація часу між надходженнями RTP-пакетів
• середня затримка RTP-пакетів.

В деяких випадках, таких як несправність порту, що бере участь в з'єднанні, або відсутність ресурсів для підтримки існуючого з'єднання, шлюз повинен сам ініціювати руйнування з'єднання за допомогою команди DeleteConnection, яка має наступний вигляд:

RetumCode
<- DeleteConnection (Calllld
Endpointid, Connectionid, Reason-code, Connection-parametera)

У параметрі Reason-code указується причина, по якій шлюз передає дане повідомлення. Решта параметрів була описана раніше.

Щоб одержати інформацію про статус якого-небудь порту шлюзу, пристрій, що управляє, може передати запит **Audit EndPoint**, який має наступний вигляд:

RetumCode
EndPointIdLietl{ [RequestedEvente] [DigitMap] [SignalRequests] [Requestldentifier,1 [NotifiedEntity] [Connectionldentifiers] [DetectEvents] [ObservedEvents] [EventStates] [Bearer Information,1 [RestartReason] [RestartDelay] [ReasonCode] [Capabilities]}
<- AuditEndPoint(Endpointid [Requestedlnfo])

Requestedlnfo - необов'язковий параметр, що описує інформацію, яку запрошує пристрій управління.

У відповідь на команду AuditEndPoint шлюз повертає необхідну інформацію (якщо ніякій інформації не запрошується, але вказаний в команді порт існує, то шлюз просто повертає підтвердження). Відповідає можуть міститися наступні параметри:

SignalRequests - необов'язковий параметр, в якому указується список сигналів, що обробляються зараз;

Observed Events - необов'язковий параметр, в якому приводиться поточний список виявлених подій;

RestartReason - необов'язковий параметр, в якому міститься причина рестарту порту, вказана в останній переданій шлюзом команді RestartlnProgress;

RestartDelay - необов'язковий параметр, в якому міститься величина затримки рестарту, вказана в останній переданій шлюзом команді RestartlnProgress;

Capabilities - необов'язковий параметр, що містить таку ж інформацію, як і параметр LocalConnectionOptions.

За допомогою команди **AuditConnection** пристрій управління запрошує параметри з'єднання, в якому бере участь порт шлюзу.

Команда має наступний вигляд:

ReturnCode [Calllld]
[NotifiedEntity] [LocalConnectionOptione] [Mode]
[RemoteConnectionDescriptor] [LocalConnectionDescriptor] [ConnectionParameters]
<- AuditConnection (Endpointid
Connectionid
Requestedlnfo)

Всі параметри команди вже були описані раніше. Якщо ніякої інформації не вимагається і вказаний порт існує, то шлюз перевіряє, що з'єднання існує, і повертає підтвердження.

Команда **RestartinProgress** передається шлюзом для індикації того, що один або група портів виводяться з робочого стану або повертаються в робочий стан. Дана команда має наступний вигляд:

ReturnCode [NotifiedEntity] <-- RestartinProgress (EndPointId
RestartMethod [RestartDelay] [Reason-code])

Параметр RestartMethod специфікує вид рестарту. Визначено декілька видів рестарту:

• Graceful restart - поступовий рестарт, при якому порти устаткування виводяться з обслуговування після певної затримки. Встановлені з'єднання не руйнуються, але і нові не створюються.

• Forced restart - примусовий рестарт, при якому руйнуються встановлені з'єднання.

• Restart - рестарт, при якому порт устаткування повертається в обслуговування після певної затримки. При цьому порт у момент рестарту не бере участь ні в яких з'єднаннях.

• Disconnected - дане значення привласнюється параметру Restart-Method, коли порт знаходився поза обслуговуванням, але в даний момент намагається повернутися в обслуговування.

• Cancel-graceful - дане значення привласнюється параметру Re-startMethod, коли шлюз відміняє передуючу команду Restart з параметром RestartMethod, якому було привласнене значення Graceful.

Параметр RestartDelay визначає затримку рестарту в секундах.

По аналогії з попередніми главами в таблицю 4.1 зведені всі команди протоколу MGCP.

Таблиця 4.1 Команди протоколу MGCP

Команда	Напрям передачі	Призначення
EndpointConfiguration (Конфігурація порту)	CA -> MG	Call Agent інструктує шлюз, яким чином йому потрібно обробляти одержувані мовні сигнали
CreateConnection (Створити з'єднання)	CA -> MG	Call Agent дає вказівку шлюзу створити з'єднання
ModifyConnection (Модифікувати з'єднання)	CA -> MG	Call Agent дає вказівку шлюзу змінити параметри існуючого з'єднання
DeleteConnection (Завершити з'єднання)	CA -> MG, MG -> CA	Call Agent і шлюзи завершують з'єднання
NotificationRequest (Запит повідомлення)	CA -> MG	Call Agent інструктує шлюз, які події необхідно виявляти.
Notify (Повідомити)	MG -> CA	Шлюз інформує Call Agent про те, що відбулося подія з числа тих, які були специфіковані в команді NotificationRequest
AuditEndpoint (Перевірити порт)	CA -> MG	Call Agent запрошує інформацію про який-небудь порт шлюзу
AuditConnection (Перевірити з'єднання)	MGC -> MG	Call Agent запрошує параметри з'єднання
ReStartlnProgress (Йде рестарт)	MG -> MGC	Шлюз інформує Call Agent про те, що один або декілька портів виводяться з робочого стану або повертаються в робочий стан

4.5 Структура команд

Команда протоколу MGCP обов’язково вміщує заголовок, за которым може йти опис сеансу зв’язку (session description). Заголовок команди та опис сеансу зв’язку являють собою набір текстових строк. Опис сеансу вітділено від заголовка команди пустой строкою.

Заголовок вміщує список параметрів и командну строку виду **CRCX 1204 ts/1@protei.loniis.net MGCP 0.1.** Командна строка, в свою чергу, складається з декількох інформаційних полів:

1. *Назва команди* дана у вигляді коду з чотирьох букв (табл.4.2)

Таблиця 4.2 Кодировка команд протоколу MGCP

Команда	Код
EndpointConfiguration	EPCF
CreateConnection	CRCX
ModifyConnection	MDCX
DeleteConnection	DLCX
NotificationRequest	RQNT
Notify	NTFY
AuditEndpoint	AUEP
AuditConnection	AUCX
ReStartlnProgress	RSIP

2. Ідентификатор транзакції. Протокол MGCP передбачає кореляцію команд і відповідей. Команда і відповідь на неї утворюють транзакцію, яка має унікальний ідентифікатор (Transaction-Identifier). Ідентифікатор транзакції вміщується в заголовок і команди, і відповіді. Значення ідентифікаторів вибираються з діапазону чисел 1 -999999999, причому значення ідентифікатора поточної транзакциії на одиницю більше ідентифікатора попередньої транзакції.

3. *Ідентифікатор порта* визначає тот порт шлюза, якому належить виконати команду, за виключенням команд Notify и ReStartlnProgress, в яких ідентифікатор визначає порт, який передав команду. Ідентифікатори портов кодуються так само, как кодуються адреса електронної пошти в відповідності з документом RFC 821 комітета IETF. Наприклад, можливий ідентифікатор ts/1@protei.loniis.net, який ідентифікує перший порт (временной канал) шлюза «protei», розташованого в домені loniis.

4. *Версія протокол* кодуеться наступним чином: MGCP 1.0.

Вище вказувалося, що заголовок команди, крім командної строки, вміщує список параметрів. Параметри команд протоколу MGCP зведені в таблицю 4.3.

Таблиця 4.3 Параметри команд протоколу MGCP

Назва параметра	Код	Опис і значення параметра
ResponseAck (Підтвердження транзакції)	К	Підтверджує завершення однієї або декількох транзакцій. Наприклад, параметр До: 6234-6255, 6257, 19030-19044 підтверджує завершення транзакцій, що мають ідентифікатори з 6234 по 6255, 6257 і з 19030 по 19044.
Bearerlnformation (Відомості про вид інформації)	В	Служить для доставки інформації про закон кодування мовної інформації А або m
ReasonCode (Код причини)		Визначені наступні коди причини; 000 - номінальний стан порту, передається тільки відповідає на запит про стан порту 900 - несправність порту 901 - порт виведений з обслуговування 902 - відмова на фізичному рівні (наприклад, втрата синхронізації)
CalllD (Ідентифікатор сеансу зв'язку)	С	Ідентифікує сеанс зв'язку, в якому може використовуватися одне або декілька з'єднань. Ідентифікатор кодується шестнадцятерічною послідовністю символів завдовжки не більше 32 символом.
ConnectionID (Ідентифікатор підключення)	1	Ідентифікує підключення даного порту до одного з'єднання, оскільки один порт може бути одночасно підключений до декількох з'єднань
Notified Entity (Об'єкт, що повідомляється)	N	Ідентифікатор об'єкту, до якого слід передавати повідомлення про виявлені події. Якщо даний параметр опущений, порт передає цю інформацію до об'єкту, від якого була одержана команда. Ідентифікатор об'єкту кодується так само, як кодуються адреси електронної пошти згідно RFC 821, наприклад MGC@ca.anynet.com:5625 або Joe@[128.23.0.4]. При використанні IP-адреси, він повинен бути поміщений в квадратні дужки.
Requestldentifier (Ідентифікатор запиту)	X	Погоджує вимогу повідомити про подію, одержане від Call Agent, з повідомленням, передаваним шлюзом в команді Notify.
LocalConnection Options (Параметри підключення порту до з'єднання)	L	Дані про алгоритм кодування інформації, розмір мовних пакетів в мс, використовувану смугу пропускання в Кбит/с, типі обслуговування, використанні ехокомпенсациі і інші відомості. Передається від Call Agent до шлюзу, звичайно в команді CRCX.

ConnectionMode (Режим з'єднання)	M	Визначені наступні режими з'єднання: передача, прийом, прийом/передача, конференція, передача даних, відсутність активності, петля, тест і інші режими. Значення параметру привласнює Call Agent.
RequestedEvents (Запрошувані події)	R	Список подій, про які слід оповістити Call Agent, і дії шлюзу при виявленні події. Визначені наступні дії: оповістити Call Agent про подію негайно; чекати подальших подій; якщо подією є прийом сигналу DTMF, то накопичувати цифри відповідно до вимог параметра DigitMap; у певних ситуаціях передавати в канал акустичні або зухвалі сигнали; обробити інкапсульовану команду Endpoint Configuration, ігнорувати подію і ін.
SignalRequests (Вимога передати сигнал)	S	Специфікується сигнал, який повинен бути переданий абоненту, наприклад, акустичний сигнал "Відповідь станції".
DigitMap (План нумерації)	D	Специфікує правила обробки сигналів DTMF. При накопиченні кількості цифр, вказаної в даному параметрі, шлюз повинен передати їх пристрою управління.
ObservedEvents (Виявлені події)	0	Список виявлених подій.
ConnectionParameters (Параметри з'єднання)	P	Статистичні дані про з'єднання, що передаються шлюзом після його завершення.
SpecifiedEndPointID (Ідентифікатор порту)	Z	Ідентифікатор порту у форматі RFC821, наприклад EndPoint@hub1 .anynet.com:5625,
Requestedlnfo (Запрошувана інформація)	F	Описує інформацію, яку Call Agent запрошує у шлюзу, наприклад, цифри номера абонента, що викликається, набрані зухвалим абонентом.
QuarantineHandling (Карантинна обробка)	Q	Визначає правила обробки подій, які були виявлені до отримання даної команди в період так званого карантину (quarantine period), і про які Call Agent ще не був оповіщений.
3DetectEvents (Події, що виявляються)	T	Перелік подій, які порт повинен відстежувати, а при їх виявленні - сповіщати про це Call Agent.
EventStates (Стани,	ES	Перелік станів порту, обумовлених, наприклад, тим, що абонент зняв або поклав трубку; інформація про ці

обумовлені подіями)		стани повинна передаватися до Call Agent у відповідь на команду AuditEndpoint.
RestartMethod (Метод рестарту)	RM	Спосіб індикації шлюзом виведення порту з обслуговування або введення його в обслуговування. Підтримуються декілька варіантів рестарту: "graceful", "forced", "restart", "disconnected" or "cancel-graceful".
RestartDelay (Затримка рестарту)	RD	Визначає час в секундах, після якого проводиться проводиться порту. Якщо цей параметр відсутній, затримка рестарту рівна нулю. При отриманні від Call Agent вимоги про примусовий рестарт порту команда виконується негайно.
Capabilities (Функціональні можливості порту)	A	Інформацію про функціональні можливості порту запрошує Call Agent за допомогою команди AuditEndpoint. Ці можливості порту включають: підтримувані алгоритми кодування, період пакетізації, смугу пропускання, ехокомпенсацию, придушення пауз мови, режими з'єднання, тип обслуговування, сукупність подій і ін.

Не всі параметри, наведені в таблиці 4.3, повинні бути обов'язково присутніми у всіх командах протоколу MGCR В таблиці 4.4 представлені можливі комбінації параметрів в командах протоколу MGCR Буква М означає обов'язкову присутність параметра в команді, буква О - не обов'язкова присутність, буква F забороняє присутність параметра.

Таблиця 4.4 Комбінації параметрів в командах протоколу MGCP

Ім'я параметра	EP CF	CR CX	MD CX	DL CX	RQ NT	NT FY	AU EP	AU CX	RS IP
ResponseAck	0	0	0	0	0	0	0	0	0
Bearerlnformation	M	0	0	0	0	F	F	F	F
Calllld	F	M	M	0	F	F	F	F	F
Connectionid	F	F	M	0	F	F	F	M	F
Requestldentifier	F	0**	o**	o**	M	M	F	F	F
LocalConnection	F	0	0	F	F	F	F	F	F
Options									
Connection Mode	F	M	M	F	F	F	F	F	F
Requested Events	F	0	0	0	O*	F	F	F	F
SignalRequests	F	0	0	0	O*	F	F	F	F
NotifiedEntity	F	0	0	0	0	0	F	F	F
ReasonCode	F	F	F	0	F	F	F	F	0
Observed Events	F	F	F	F	F	M	F	F	F

DigitMap	F	0	0	0	0	F	F	F	F
Connection	F	F	F	0	F	F	F	F	F
Parameters									
Specific Endpoint ID	F	F	F	F	F	F	F	F	F
Second Endpoint ID	F	0	F	F	F	F	F	F	F
Requestedlnfo	F	F	F	F	F	F	M	M	F
QuarantineHandling	F	0	0	0	0	F	F	F	F
DetectEvents	F	0	0	0	0	F	F	F	F
EventStates	F	F	F	F	F	F	F	F	F
RestartMethod	F	F	F	F	F	F	F	F	M
RestartDelay	F	F	F	F	F	F	F	F	0
SecondConnectionID	F	F	F	F	F	F	F	F	F
Capabilities	F	F	F	F	F	F	F	F	F
RemoteConnection	F	0	0	F	F	F	F	F	F
Descriptor									
LocalConnection	F	F	F	F	F	F	F	F	F
Descriptor									

** - параметр Requestldentifier не обов'язковий для команд Create-Connection, ModifyConnection і DeleteConnection, але якщо ці команди містять інкапсульовану команду NotificationRequest, присутність в них параметра Requestldentifier стає обов'язковою;

* - параметри Requested Events і SignalRequests не обов'язкові для команди NotificationRequest

.

4.6 Структура відповідей на команди

Протокол MGCP передбачає підтвердження отримання всіх команд. Структура відповідей на команди в протоколі MGCP ідентична вищеописаній структурі самих команд. Відповідь на команду також є набором текстових рядків і обов'язково містить заголовок відповіді, за якою (після порожнього рядка) може слідувати опис сеансу зв'язку.

У цьому параграфі мова піде, головним чином, про заголовок відповіді. Заголовок складається з у відповідь рядка, наприклад, **2001203 OK,** і списку параметрів. У відповідь рядок, у свою чергу, складається з декількох інформаційних полів: коду відповіді, ідентифікатора транзакції і необов'язкового коментаря.

У таблиці 4.5 приведені можливі варіанти коду відповіді на команди протоколу MGCP.

Таблиця 4.5 Коди відповідей на команди протоколу

Код	Значення коду
100	Одержана команда в даний момент обробляється, повідомлення про виконання команди буде передано пізніше
200	Одержана команда виконана
250	З'єднання зруйноване
400	Транзакція не може бути виконана із-за тимчасової помилки
401	Трубка телефону вже знята
402	Трубка телефону вже повішена
403	Команда не може бути виконана через відсутність в даний момент необхідних ресурсів
404	Зараз відсутня необхідна смуга пропускання
500	Команда не може бути виконана, тому що порт невідомий
501	Команда не може бути виконана, тому що порт не готовий до її виконання
502	Команда не може бути виконана, тому що порт не має необхідної смуги пропускання
510	Команда не може бути виконана із-за помилки в протоколі
511	Команда не може бути виконана, оскільки в ній міститься нерозпізнане розширення
512	Команда не може бути виконана, тому що шлюз не має засобів детектування одного із запрошуваних сигналів
513	Команда не може бути виконана, тому що шлюз не має засобів генерування одного із запрошуваних сигналів
514	Команда не може бути виконана, тому що шлюз не може передати необхідне мовне повідомлення або підказку
515	Команда має некоректний ідентифікатор з'єднання, наприклад, ідентифікатор вже завершеного з'єднання
516	Команда має некоректний ідентифікатор сеансу зв'язку
517	Непідтримуваний або некоректний режим
518	Непідтримувана або невідома сукупність сигналів або подій
519	Порт не має відомостей про план нумерації
520	Команда не може бути виконана, тому що йде рестарт порту
521	Порт переданий іншому Call Agent
522	Немає такої події або сигналу
523	Невідома дія або недозволена комбінація дій
524	Внутрішня невідповідність в параметрі LocalConnectionOptions
525	Невідоме розширення параметра LocalConnectionOptions
526	Недостатня смуга пропускання
527	Відсутній параметр LocalConnectionOptions
528	Несумісна версія протоколу

529	Відмова в апаратному забезпеченні
530	Помилка в сигнальному протоколі CAS
531	Відмова групи каналів або трактів

З представленого в таблиці 4.5 переліку кодів відповідей видно, що їх основна роль полягає в захисті від помилок протоколу, конфігурації або функціональних можливостей. На підставі інформації, що надається цими кодами помилок, неможливо реалізувати осмислений механізм діагностики. Для отримання діагностичної інформації від шлюзів і портів шлюзу потрібні інші методи. Одним з можливих методів є протокол SNMP (простий протокол експлуатаційного управління мережею), який, безумовно, знайде застосування в транспортних шлюзах IP-телефонії.

На закінчення розгляду структури відповідей на команди протоколу MGCP приведемо можливі комбінації параметрів у відповідях (таблиця 4.6).

Таблиця 4.6 Можливі комбінації параметрів у відповідях протоколу MGCP

Им’я параметра	EP CF	CR CX	MD CX	DL CX	RQ NT	NT FY	AU EP	AU CX	RS IP
ResponseAck	F	F	F	F	F	F	F	F	F
Bearerlnformation	F	F	F	F	F	F	0	F	F
Calllld	F	F	F	F	F	F	F	0	F
Connectionid	F	0	F	F	F	F	F	F	F
Requestldentifier	F	F	F	F	F	F	0	F	F
LocalConnection	F	F	F	F	F	F	0	0	F
Options									
Connection Mode	F	F	F	F	F	F	F	0	F
RequestedEvents	F	F	F	F	F	F	0	F	F
SignalRequests	F	F	F	F	F	F	0	F	F
Notified Entity	F	F	F	F	F	F	F	F	0
ReasonCode	F	F	F	F	F	F	0	F	F
Observed Events	F	F	F	F	F	F	0	F	F
DigitMap	F	F	F	F	F	F	0	F	F
Connection	F	F	F	0	F	F	F	0	F
Parameters									
Specific Endpoint ID	F	0	F	F	F	F	F	F	F
Requested Info	F	F	F	F	F	F	F	F	F
QuarantineHandlin g	F	F	F	F	F	F	0	F	F
DetectEvents	F	F	F	F	F	F	0	F	F
EventStates	F	F	F	F	F	F	0	F	F

RestartMethod	F	F	F	F	F	F	0	F	F
RestartDelay	F	F	F	F	F	F	0	F	F
Capabilities	F	F	F	F	F	F	0	F	F
SecondConnection Id	F	0	F	F	F	F	F	F	F
SecondEndpointID	F	0	F	F	F	F	F	F	F
LocalConnection	F	м	0	F	F	F	F	0	F
Descriptor									
RemoteConnection	F	F	F	F	F	F	F	0	F
Descriptor									

4.7 Описи сеансів зв'язку

При встановленні з'єднань Call Agent надає портам шлюзів, що беруть участь в цих з'єднаннях, необхідну інформацію один про одного - опис сеансів зв'язку. Опис сеансу зв'язку вводиться до складу деяких команд і відповідей протоколу MGCP і включає IP-адресу, UDP/RTP порт, вид інформації, алгоритм кодування інформації, розмір мовних пакетів і т.д. Синтаксис опису сеансу зв'язку в протоколі MGCP відповідає синтаксису протоколу опису сеансів зв'язку - session description protocol (SDP), запропонованому для використання у вищезгаданих цілях комітетом IETF в документі RFC 2327 [53].

Протокол SDP може застосовуватися для опису мультимедійних конференцій, але поточна версія протоколу MGCP використовує протокол SDP тільки для опису параметрів передачі мови і даних.

Оскільки робота присвячена аналізу технології передачі мовної інформації по мережах з маршрутизацією пакетів IP, в даному параграфі ми розглянемо синтаксис протоколу SDP тільки в частині опису сеансу мовного зв'язку. Для опису такого сеансу в протоколі SDP передбачено декілька інформаційних полів:

• *Версія протоколу SDP.* Поточна версія протоколу - нульова. Поле кодується таким чином: v=0.

• *IP-адреса шлюзу.* Це поле містить IP-адресу, яка використовуватиметься для обміну пакетами RTP. Якщо це поле включене в команди протоколу MGCP, то воно означає адресу видаленого шлюзу, якщо поле включене у відповіді, то - адреса шлюзу, що передає відповідь.

• *Поле опису мовного каналу.* Дане поле містить індикацію виду передаваної або такої, що приймається інформації (у нашому випадку - мови), номер порту, використовуваного для прийому RTP пакетів видаленим шлюзом (якщо поле опису мовного каналу включене в команди протоколу MGCP) або локальним шлюзом (якщо це поле включене у відповіді), індикацію використання протоколу RTP для передачі мови і алгоритми кодування мовної інформації. Поле кодується буквою т.

• *Режим з'єднання.* Режими з'єднань представлені в таблиці 4.7.

Таблиця 4.7 Режими з'єднання

Кодировка режима	Функціонування шлюзу
sendonly	Шлюзу належить тільки передавати інформацію
recvonly	Шлюзу належить тільки приймати інформацію
sendrecv	Шлюзу належить передавати і приймати інформацію
inactive	Шлюз не повинен ні передавати, ні приймати інформацію
loopback	Шлюз повинен передавати інформацію, що приймається, у зворотному напрямі
contest	Шлюзу належить перевести порт в режим тестування

Окрім вищезгаданих полів, для опису сеансу мовного зв'язку в протоколі SDP передбачено ще декілька необов'язкових інформаційних полів. Відзначимо, що якщо в команду або у відповідь протоколу MGCP включені описи декількох сеансів зв'язку, то вони відділяються один від одного рядком з вказівкою версії протоколу SDP. Типовий приклад опису сеансу мовного зв'язку з використанням протоколу SDP приведений нижче:

v = Про

з = IN IP4 128.96.41.1

m = audio 3456 RTP/AVP 0

Даний приклад заслуговує короткого коментаря. Для опису сеансу зв'язку використовується протокол SDP, версія 0, в мережі використовується протокол IP, версія 4, IP адреса шлюза- 128.96.41.1, передається або приймається мовна інформація, упакована в пакети RTP, номер порту RTP - 3456, алгоритм кодування мови G.711.

4.8 Встановлення, зміна і руйнування з'єднань

У даному параграфі буде показано, яким чином за допомогою протоколу MGCP встановлюються, змінюються і завершуються мовні з'єднання в мережах з маршрутизацією пакетів IP. Приклад охоплює взаємодію протоколу MGCP з протоколом ОКС7 (рис. 4.6).

Від телефонної станції АТС1 до шлюзу сигналізації SG1 по загальному каналу сигналізації поступає запит з'єднання - повідомлення IAM. Шлюз SG1 передає повідомлення IAM пристрою управління шлюзами Call Agent, яке обробляє запит і визначає, що виклик повинен бути направлений до телефонної станції АТС2 за допомогою шлюзу TGW2.

Далі Call Agent резервує порт шлюзу TGW1 (розмовний канал). З цією метою Call Agent передає шлюзу команду CreateConnec-tion. Відзначимо, що порт шлюзу TGW1 може тільки приймати інформацію (режим recvonly), оскільки він ще не обізнаний про те, на яку адресу і яким чином йому слід передавати інформацію.

CRCX 1204 trunk-group-l/17@tgwl.whatever.net MGCP 0.1

C : A3C47F21456789FO

L: p:10, a:G.711

M: recvonly

Відповідає на прийняту команду шлюз TGW1 повертає опис сеансу зв'язку.

200 1204 OK
I:FDE234C8
v=0
C=IN IP4 128.96.41.1
m=audio 3456 RTP/AVP 0

Після прийому від шлюзу TGW1 підтвердження Call Agent передає команду CRCX другому шлюзу TGW2 з метою зарезервувати в ньому порт:

CRCX 1205 trunk-group-2/$@tgw2.whatever.net MGCP 0.1
C : A3C47F21456789FO
M: sendrecv
v0
C=IN IP4 128.96.41.1
m=audio 3456 RTP/AVP 0

Шлюз TGW 2 вибирає порт, який братиме участь в зв'язку, і підтверджує прийом команди CRCX.

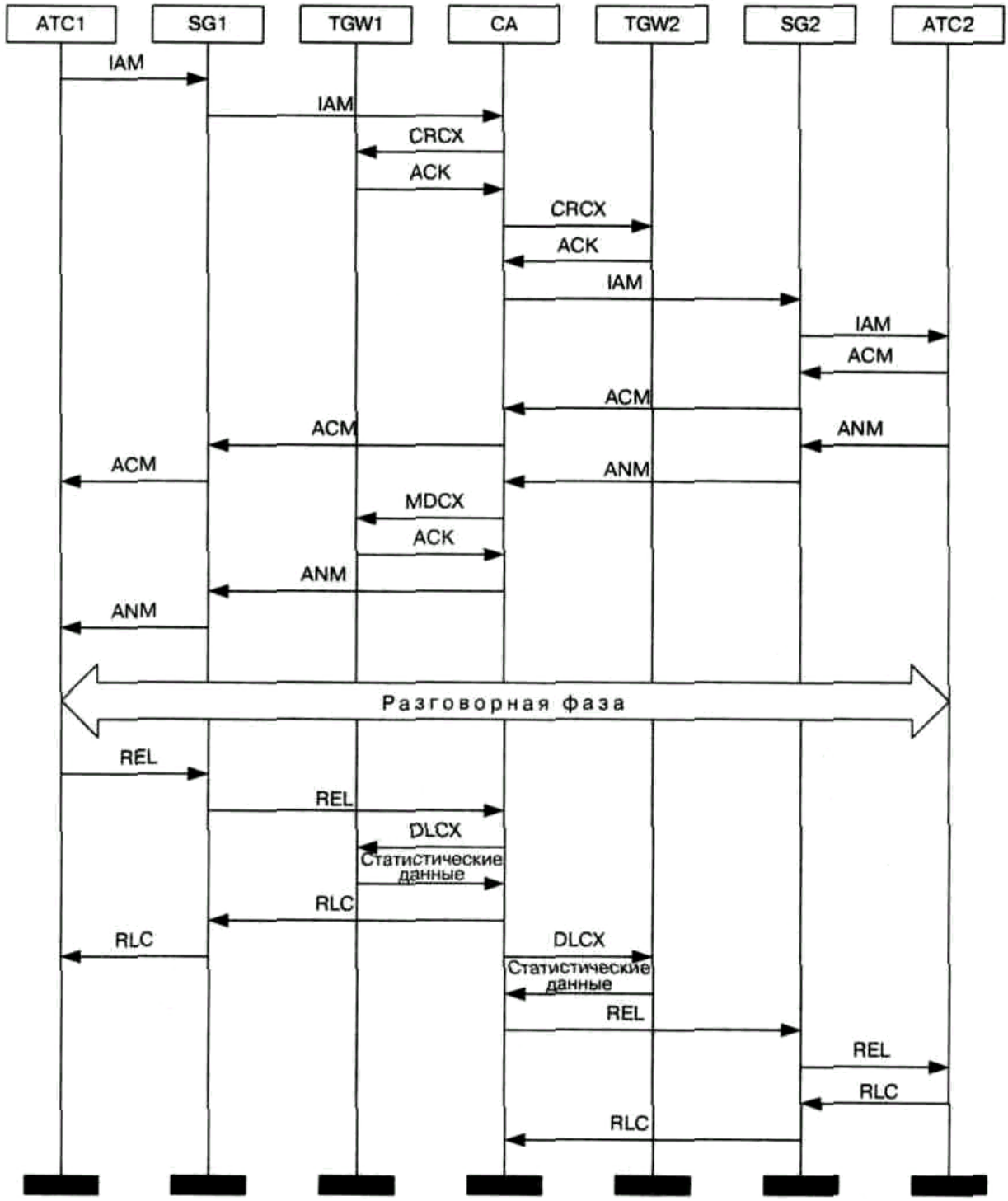


Рисунок 4.6 Встановлення і руйнування з'єднання з використанням протоколу MGCP

200 1205 OK
I:abc0
v=0
C-IN IP4 128.96.63.25
m=audio 1296 RTP/AVP 0

За допомогою двох команд CRCX створюється односпрямований розмовний канал для передачі абоненту акустичних сигналів або мовних підказок і сповіщень, що викликається. В той же час, порт шлюзу TGW 2 вже може не тільки приймати, але і передавати інформацію, оскільки він одержав опис сеансу зв'язку від стрічного шлюзу. Далі Call Agent передає повідомлення 1AM до телефонної станції АТС2. На повідомлення 1AM станції АТС2 відповідає повідомленням АСМ, яке негайно пересилається до станції АТС1.

Після того, як абонент, що викликається, прийме виклик, телефонна станція АТС2 передає до Call Agent повідомлення ANM. Далі Call Agent змінює режим з'єднання recvonly в шлюзі TGW1 на повнодуплексний режим:

MDCX 1206 trunk-group-I/17@tgwl.whatever.net MGCP 0.1
C : A3C47F21456789FO
I: FDE234C8
M: sendrecv
v=0
C=IN IP4 128.96.63.25
m=audio 1296 RTP/AVP 0

Шлюз TGW1 виконує і підтверджує зміну режиму з'єднання:

200 1206 OK

Call Agent передає повідомлення ANM до телефонної станції АТС1, після чого наступає розмовна фаза з'єднання.

Завершення розмовної фази відбувається таким чином. У нашому випадку абонент, що викликав, дає відбій першим, телефонна станція АТС1 через шлюз сигналізації передає до Call Agent повідомлення REL. На підставі цього повідомлення Call Agent завершує з'єднання з абонентом, що викликав:

DLCX 1207 trunk-group-I/17&tgwl.whatever.net MOCP 0.1
З: A3C47F21456789FO I:FDE234C8

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

250 1217 OK
P : PS-1245, OS-62345, PR-780, OR'45123, PL-10, JI-27,LA=48

Далі Call Agent передає до АТС1 повідомлення RLC з метою підтвердити руйнування з'єднання.

Паралельно Call Agent завершує з'єднання з викликаною стороною:

DLCX 1208 trunk-group-2/13@tgw2.whatever.net MGCP 0.1
З: A3C47F21456789FO
I:abc0

Шлюз TGW2 підтверджує завершення з'єднання і передає до Call Agent зібрані за час з'єднання статистичні дані

250 1218 OK
P : PS=790, 08=45700 PR=1230, OR=61875, PL=15, JI=27,IA=48

Після прийому відповіді на команду DLCX Call Agent може починати процедуру завершення з'єднання з АТС2, яка повинна підтвердити роз'єднання, після чого з'єднання вважається зруйнованим.

4.9 Можливості і перспективи протоколу MGCP

Для побудови добре функціонують і сумісних з ТФОП мереж IP-телефонії сьогодні підходять протоколи H.323 і MGCP. Підхід з використанням MGCP володіє вельми важливою перевагою перед підходом, запропонованим ITU в рекомендації H.323: Call Agent підтримує сигналізацію ОКС7 і інші види телефонної сигналізації; підтримується також прозора трансляція сигнальної інформації по мережі IP-телефонії. У мережі, побудованій на базі рекомендації H.323, сигналізація ОКС7, як і будь-яка інша сигналізація, повинна конвертуватися шлюзом в сигнальні повідомлення H.225.0 (Q.931).

В цілому ж, аналізуючи функціональні можливості протоколу MGCP, можна зробити наступний висновок: протокол, пропонований робочою групою MEGACO організації IETF, краще за інших підходить для розгортання глобальних мереж IP-телефонії, що приходять на зміну традиційним телефонним мережам.

Але, в той же час, слід зазначити, що в існуючих сьогодні додатках IP-телефонії, таких як надання послуг міжнародного і міжміського зв'язку, використовувати протокол MGCP (так само, як і протокол SIP) недоцільно у зв'язку з тим, що переважна більшість мереж IP-телефонії сьогодні побудована на базі протоколу H.323. Оператору доведеться будувати на базі протоколу MGCP (або SIP) окрему мережу IP-телефонії, що зажадає значних капіталовкладень, тоді як оператор зв'язку, що має устаткування стандарту H.323, може легко приєднати свою мережу до існуючих мереж.

5. ПОРІВНЯЛЬНИЙ АНАЛІЗ ПРОТОКОЛІВ H.323, SIP та MGCP.

Протоколи H.323 та SIP являють собою досить різний підхід до вирішення одних і тих же задач. Протокол H.323, котрий створювався фахівцями ITU-T виявився ближче до традиційних телефонних мереж, тоді як рішення комітету IETF, котрий займався розробкою протоколу SIP, реалізує більш простий підхід на основі HTTP.

Також слід зазначити, що протокол H.323 є старшим, а значить досвід використання його в роботі – більшим. Існує ще один момент, на який варто звернути увагу. Інтенсивне впровадження технології передачі мовної інформації через IP-мережі привело до постійного нарощування функціональних можливостей як протоколу H.323, так і протоколу SIP. В результаті переваги одного з протоколів переймаються іншим.

Протокол MGCP стоїть дещо осторонь протоколів H.323 та SIP, адже, на відміну від них, MGCP використовується тільки для зв'язку між шлюзами та пристроєм керування Call Agent. Тому не можна порівнювати за всіма критеріями протокол MGCP та H.323 чи SIP. Хоча в таких питаннях, як масштабованість мережі чи підтримка сигналізації ТМЗК порівняти всі три протоколи ніщо не заважає.

Основними критеріями, якими можна характеризувати протоколи сигналізації даного типу є:

- масштабованість мережі;
- розширюваність протоколу;
- підтримка сигналізації ТМЗК;
- час встановлення з'єднання;
- складність протоколу;
- адресація;
- персональна мобільність користувачів;
- додаткові послуги;

Приведені критерії дозволяють характеризувати протокол як зі сторони проектування та експлуатації так і зі сторони використання їх звичайним користувачем.

5.1. Масштабованість мережі.

H.323. Мережа побудована за рекомендацією H.323 має зонову архітектуру. Gatekeeper виконує функції керування однією зоною, в яку входять: термінали, шлюзи, пристрої керування конференцією, зареєстровані в даного gatekeeper. Окремі фрагменти зони мережі H.323 можуть бути територіально рознесеними та з'єднюватися за допомогою маршрутизаторів рис.2.2.

SIP. Мережі побудовані на протоколі SIP подібні за масштабованістю до H.323-мереереж. Проте потрібно відмітити, що SIP-сервер може не зберігати інформацію про поточні з'єднання на відміну від gatekeeper H.323. Така можливість дозволяє опрацьовувати більшу кількість вхідних викликів.

MGCP Протокол MGCP краще інших підходить для розгортання глобальних мереж IP-телефонії. Це пояснюється самою природою даного протоколу, який призначений для організації взаємодії між центральними вузлами мережі.

5.2. Розширюваність протоколу.

Безперечно важливим є забезпечення сумісності різних версій одного протоколу. Розширюваність протоколу забезпечується:

- узгодженням параметрів;
- стандартизацією кодеків;
- модульністю архітектури.

H.323. Нові функціональні можливості вводяться до протоколу H.323 за допомогою поля NonStandardParameter. Воно містить код виробника і, слідом за ним, код послуги, що дійсний тільки для цього виробника. Це дозволяє дещо розширювати послуги, проте виникають деякі проблеми. По-перше, неможливо запросити інформацію про підтримуванню певних послуг, по-друге, неможливо додати нове значення до вже існуючого параметра. Існують також проблеми, пов'язані із забезпеченням взаємодії устаткування різних виробників.

У протоколі H.323 усі кодеки повинні бути стандартизовані. Тому додатки з нестандартними алгоритмами кодування можуть зіштовхнутися з проблемами при реалізації їх на базі протоколу H.323.

Архітектура протоколу H.323 монолітна і являє собою інтегрований набір протоколів для одного застосування. Протокол складається з трьох основних складових, і для створення нової послуги може знадобитися модифікація кожної з цих складових.

SIP. Протокол SIP досить просто забезпечує сумісність різних версій. Якщо устаткування розуміє значення поля, воно приймається на виконання, тоді як незрозумілі поля просто ігноруються. Це зменшує складність протоколу, а також полегшує обробку повідомлень і впровадження нових послуг. У протоколі SIP для передачі інформації про функціональні можливості термінала використовується протокол SDP.

Значно простішою, в порівнянні з H.323, тут виглядає ситуація з кодеками. Якщо виробник підтримує якийсь особливий алгоритм кодування, то цей алгоритм просто реєструється в організації IANA.

Протокол SIP складається з набору модулів, що можуть замінятися в залежності від вимог і можуть працювати незалежно один від одного.

MGCP Загалом функції, що дозволяють розширити можливості протоколу MGCP, подібні до аналогічних функцій протоколу SIP. Це пояснюється тим, що обидва протоколи використовують один і той же синтаксис опису сеансів зв’язку – протокол опису сеансів зв’язку SDP.

5.3. Підтримка сигналізації ТМЗК.

Актуальним залишається питання про забезпечення підтримки сигналізації ТМЗК. IP-мережа, яка не підтримує встановлення з'єднання з абонентами ТМЗК, не є повноцінною.

H.323. Мережа побудована на базі рекомендації H.323 є досить близькою до традиційної телефонної мережі. Її можна розглядати як мережу ISDN, накладену на IP-мережу. Хоча потрібно відмітити, що в трьох перших версіях даного протоколу, сигналізація ТМЗК не передається прозоро, а потребує попереднього конвертування шлюзами в сигнальні повідомлення H.225.0.

SIP. SIP-мережі гірше інших стикуються з традиційними телефонними мережами. В даному, як і у випадку з протоколом H.323, сигнальні повідомлення ТМЗК повинні конвертуватися шлюзами в повідомлення SIP.

MGCP Великою перевагою протоколу MGCP є підтримка контролером шлюзів (Call Agent) сигналізації ЗКС7 та інших видів сигналізації, а також прозора трансляція сигнальної інформації по мережі IP-телефонії.

5.4. Час встановлення з'єднання.

H.323 Для встановлення з'єднання між абонентами, з використанням протоколу H.323, кінцевим терміналам необхідно обмінятися щонайменше десятком повідомлень. Спочатку, використовуючи протокол RAS, термінал получає дозвіл gatekeeper на використання мережевих ресурсів. Далі між терміналами відбувається обмін керуючими повідомленнями, які специфіковані в рекомендації H.225.0. Останнім кроком є обмін повідомленнями H.245, що дозволяють керувати інформаційними каналами. Процедура встановлення з'єднання є досить затяжною в часі, що є вагомим недоліком протоколу H.323.

SIP. На відміну від H.323 в протоколі SIP для встановлення з'єднання потрібна лише одна транзакція. У запиті INVITE міститься вся необхідна для встановлення з'єднання інформація, включаючи опис функціональних можливостей термінала. Крім того SIP може використовувати механізм багато-адресної розсилки повідомлень для пошуку абонента по декількох зареєстрованих адресах, що значно пришвидшує встановлення з'єднання.З цих причин витрати часу на встановлення з'єднання в протоколі SIP значно менші витрат часу в протоколі H.323. Правда, при використанні інкапсуляції повідомлень H.245 у повідомлення H.225 чи процедури Fast Connect час встановлення з'єднання, з використанням протоколу H.323, значно зменшується.

Крім того, на час встановлення з'єднання впливає також і транспортний протокол, що переносить сигнальну інформацію. Ранні версії протоколу H.323 передбачали використання для переносу сигнальних повідомлень H.225 і H.245 тільки протокол TCP, і лише третя версія протоколу передбачає можливість використання протоколу UDP. Протоколом SIP використання протоколів TCP і UDP передбачалося із самого початку.

Оцінка часу встановлення з'єднання виконується в умовних одиницях - RTT (round trip time) - і складає для протоколу SIP 1,5 - 2,5 RTT, а для протоколу H.323 6-7 RTT.

MGCP Якщо говорити про час встановлення з’єднння з використанням протоколу MGCP, то потрібно зазначити, що даний протокол використовується тільки для зв’язку між шлюзами та пристроєм керування. Для встановлення з’єднання між кінцевими терміналами протокол MGCP використовуватись не може. Отож в даному випадку говорячи про час встановлення з’єднання будемо мати на увазі не кінцеві термінали, а порти шлюзів.

Для встановлення з’єднання в протоколі MGCP потрібна лише одна команда – CRCX (CreateConnection). Ще ряд команд використовуються для модифікації та розірвання з’єднання, а також для керування портами та реагування на певні події. Загалом, зважаючи на вузьку спеціалізацію MGCP, час встановлення з’єднння між портами шлюзів є незначним.

5.5. Складність протоколу.

H.323 Протокол H.323, безумовно, складніший від протоколу SIP. В H.323 для організації з’єднання використовується три різні протоколи (RAS, H.225, H.245), кожен зі своїм набором повідомлень. Протокол H.323 використовує велику кількість інформаційних полів у повідомленнях, при декількох десятках таких же полів у протоколі SIP. Протокол H.323 використовує двійкові представлення своїх повідомлень, тому читати їх складніше, хоча обробка повідомлень виконується швидше.

SIP. Для організації базового з'єднання в протоколі SIP досить використовувати всього три типи запитів (INVITE, BYE і ACK). Протокол SIP використовує текстовий формат повідомлень, подібно протоколу HTTP, що полегшує синтаксичний аналіз, дає можливість ручного введення деяких полів, полегшує аналіз повідомлень.

MGCP Загалом за даним критерієм порівняння протокол MGCP подібний до протоколу SIP. Тут також використовується текстовий формат команд, а ряд параметрів, присутніх в кожній команді, є чітко визначений та легко зрозумілий.

5.6. Адресація.

H.323 У протоколі H.323 використовуються транспортні адреси та alias-адреси. У якості останнього може використовуватися телефонний номер, ім'я користувача чи адреса електронної пошти. Для перетворення alias-адреси в транспортну адресу повинен брати участь gatekeeper.

SIP. Використання URL є сильною стороною протоколу SIP і дозволяє легко інтегрувати його в існуючу систему DNS-серверів і впроваджувати в устаткування, що працює в IP-мережах. Адресою в SIP може також служити телефонний номер з адресою використовуваного шлюзу.

5.7. Персональна мобільність користувачів.

SIP. Протокол SIP має хороший набір засобів підтримки персональної мобільності абонентів. Користувач SIP-мережі може реєструвати кілька своїх адрес і вказувати пріоритетність кожної з них. В такому випадку пошук користувача буде відбуватись одночасно в декількох напрямках. При під’єднанні

до мережі кожен кінцевий термінал реєструється на сервері визначення місцеположення, що в кінцевому результаті дозволяє швидко віднайти поточну адресу користувача.

H.323 Персональна мобільність підтримується протоколом H.323, але менш гнучко. Так, наприклад, одночасний пошук користувача по декількох напрямках обмежений тим, що gatekeeper, одержавши запит визначення місця розташування користувача, не транслює його до інших gatekeeper.

5.8. Додаткові послуги.

H.323 Додаткові послуги, надані протоколом H.323, стандартизовані в серії рекомендацій ITU-T H.450.x.

Приклади послуг, наданих обома протоколами:

- Переключення з'єднання в режим утримання (Call hold);
- Переключення зв'язку (Call Transfer);
- Переадресація (Call Forwarding);
- Повідомлення про новий виклик під час зв'язку (Call Waiting);
- Конференція.

Рекомендація H.323 передбачає три способи організації конференції, проте недоліком є те, що керування конференцією у всіх випадках виконується централізовано – контролером конференцій MC (Multipoint Controller). Тому для організації конференції, по-перше, необхідна наявність контролера MC в одного з терміналів, по-друге, учасник з активним контролером MC не може вийти з конференції. Крім того, при великому числі учасників конференції MC може стати „вузьким місцем”. Перевагою протоколу H.323 у даному питанні є більш потужні засоби контролю конференцій. Протокол H.323 надає широкі можливості керування послугами, як в питаннях аутентифікації й обліку, так і в питаннях контролю використання мережних ресурсів. Можливості протоколу SIP у цій частині бідніші.

SIP. Протоколом SIP правила надання додаткових послуг не визначені, що є його серйозним недоліком, тому що викликає проблеми при організації взаємодії устаткування різних фірм-виробників.

Протокол SIP передбачає три способи організації конференції: з використанням пристрою керування конференціями MCU, режим багатоадресної розсилки та режим з'єднання учасників один з одним. В останніх двох випадках функції керування конференціями можуть бути розподілені між терміналами, тобто центральний контролер конференцій не потрібний. Це дозволяє організовувати конференції з практично необмеженою кількістю учасників. Крім того протокол SIP передбачає можливість організації зв'язку третьою стороною (third-party call control). Подібна послуга передбачена і протоколом H.323, але реалізація їх складніша.

ВИСНОВКИ

Таким чином, в дипломній роботі викладені принципи побудови мереж IP-телефонії на підставі протоколу MGCP.

На основі проведеного вище порівняння можна зробити висновок, що для розгортання глобальних мереж IP-телефонії краще інших підходить протокол MGCP.

Розглянуто, що протокол SIP більше підходить для використання Internet-провайдерам, оскільки, в такому разі послуги IP-телефонії розглядаються лише як частина набору загальних послуг.

Відповідно, що оператори телефонного зв'язку, для яких послуги Internet не є першорядними, швидше за все, будуть орієнтуватися на протокол H.323, оскільки мережа, побудована на базі рекомендації H.323, представляється їм добре знайомою мережею ISDN, накладеною на IP-мережу.

ПЕРЕЛІК ПОСИЛАНЬ

1. Гольдштейн Б.С., Пинчук А.В., Суховицкий А.Л. IP-Телефония. - М.: Радио и связь, 2001. — 336с.

2. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы. 2-е издание. – СПб.:Питер, 2005. – 864с.

3. Гольдштейн Б.С., Зарубин А.А., Саморезов В.В. Протокол SIP. Справочник – БХВ-Петербург , 2005.- 546с.

4. Ягофаров Т.М. VoIP выходит на новый виток развития./ Компьютерное Обозрение, 2002. №14.

5. Будников В.Ю., Пономарев Б.А. Технологии обеспечения качества обслуживания в мультисервисных сетях./Вестник связи, 2000. №9

6. Осадчук А.В., Матвеев С.Н. Стандарт мультимедийной связи Н.323. /Сети, 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.voip2u.ru/Techno/

11. http://cdo.bseu.by/library/ibs1/applic_l/video/h323/h323_rus

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

ДЕМОНСТРАЦІЙНІ МАТЕРІАЛИ

ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

Презентація
до магістерської кваліфікаційної роботи на ступінь
вищої освіти «магістр»
на тему: «**Дослідження можливості побудови мереж IP-телефонії на підставі протоколу MGCP»**

Виконав: студент групи ТСДМ-62, Боянов В.П.
Керівник: Лаврінець К.Г.

Мета та актуальність роботи

Мета роботи- дослідження принципів побудови мереж IP-телефонії на основі протоколів MGCP.

Актуальність. Принципи побудови мереж IP-телефонії дозволяють істотно скоротити смугу пропущення для передачі мови, відео й даних у режимі мультимедійних повідомлень і істотно знизити завдяки цьому вартість надаваних послуг абонентам.

Сімейство протоколів H.323 забезпечує можливість передачі мовних повідомлень, відео й даних по мережах IP-телефонії й добре інтегрується з можливостями ТМЗК. Протокол MGCP є більш перспективним для побудови мереж IP-телефонії оскільки він побудований на декомпозиції транспортних шлюзів, що дозволяє скоротити час передавання сигнальних повідомлень.

Галузь використання – Провайдерам Інтернет і операторам телефонного зв'язку введення IP-телефонії в спектр послуг відкриває зовсім нові ринки збуту, нових клієнтів і можливості розвитку. Корпоративним клієнтам і приватним користувачам - зниження витрат на міжміські (міжнародні) переговори, дзвінки з комп'ютера, дзвінки з Web-Сайту.

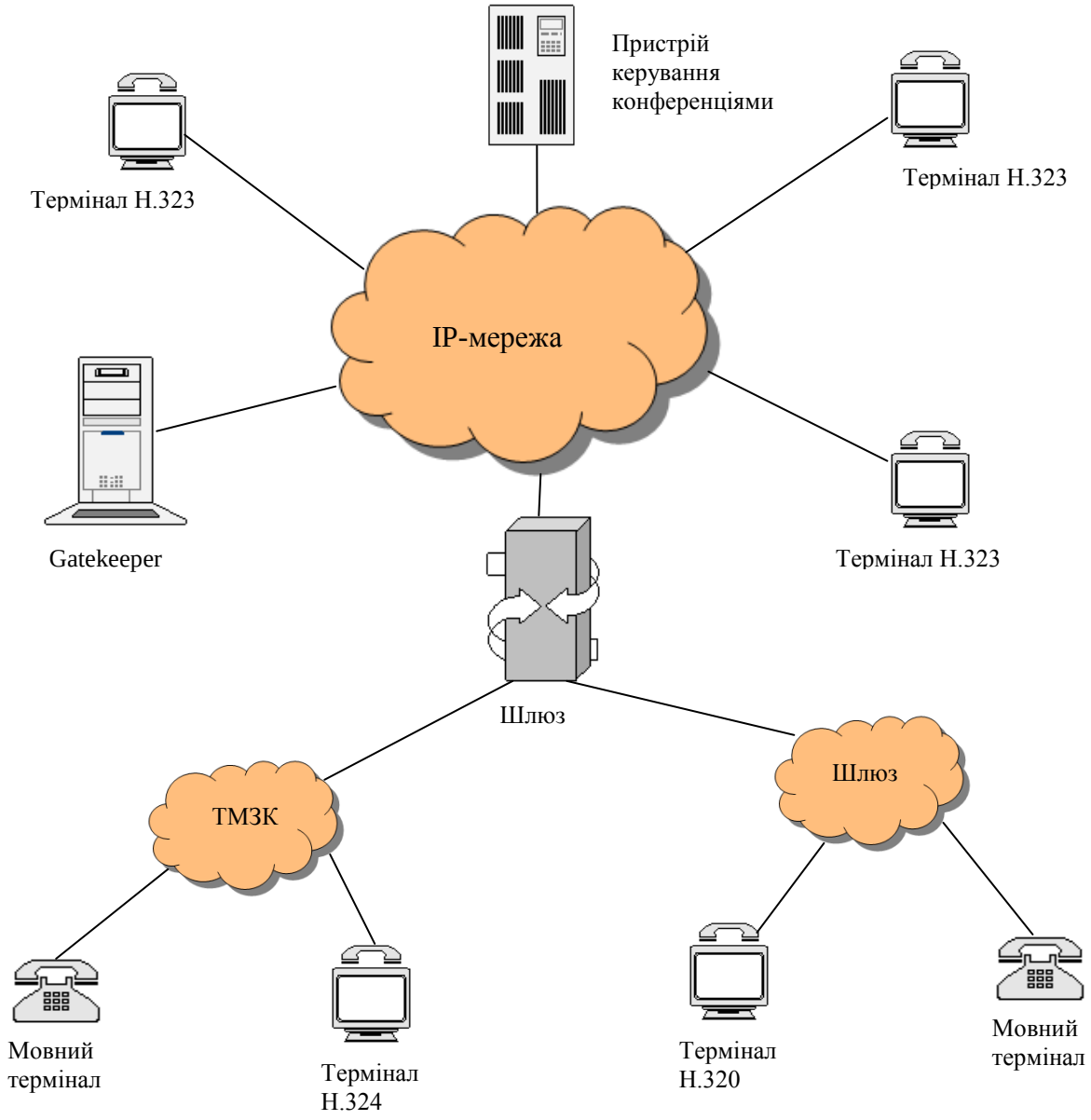
1.Команди протоколу MGCP.

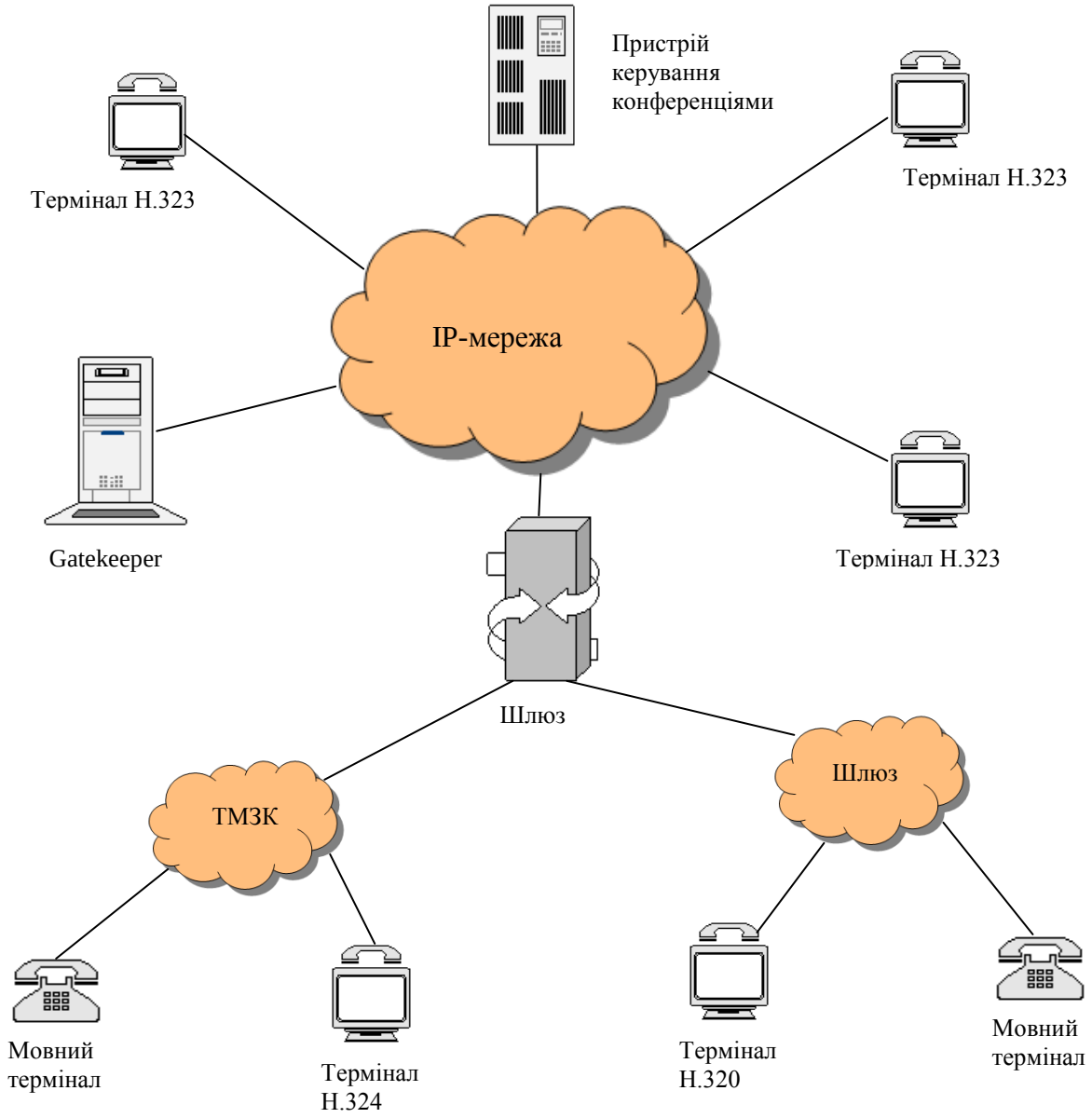
2.Архітектура мережі, що базується на протоколі MGCP.

3. Приклад встановлення і руйнування з’єднання з використанням протоколу MGCP.

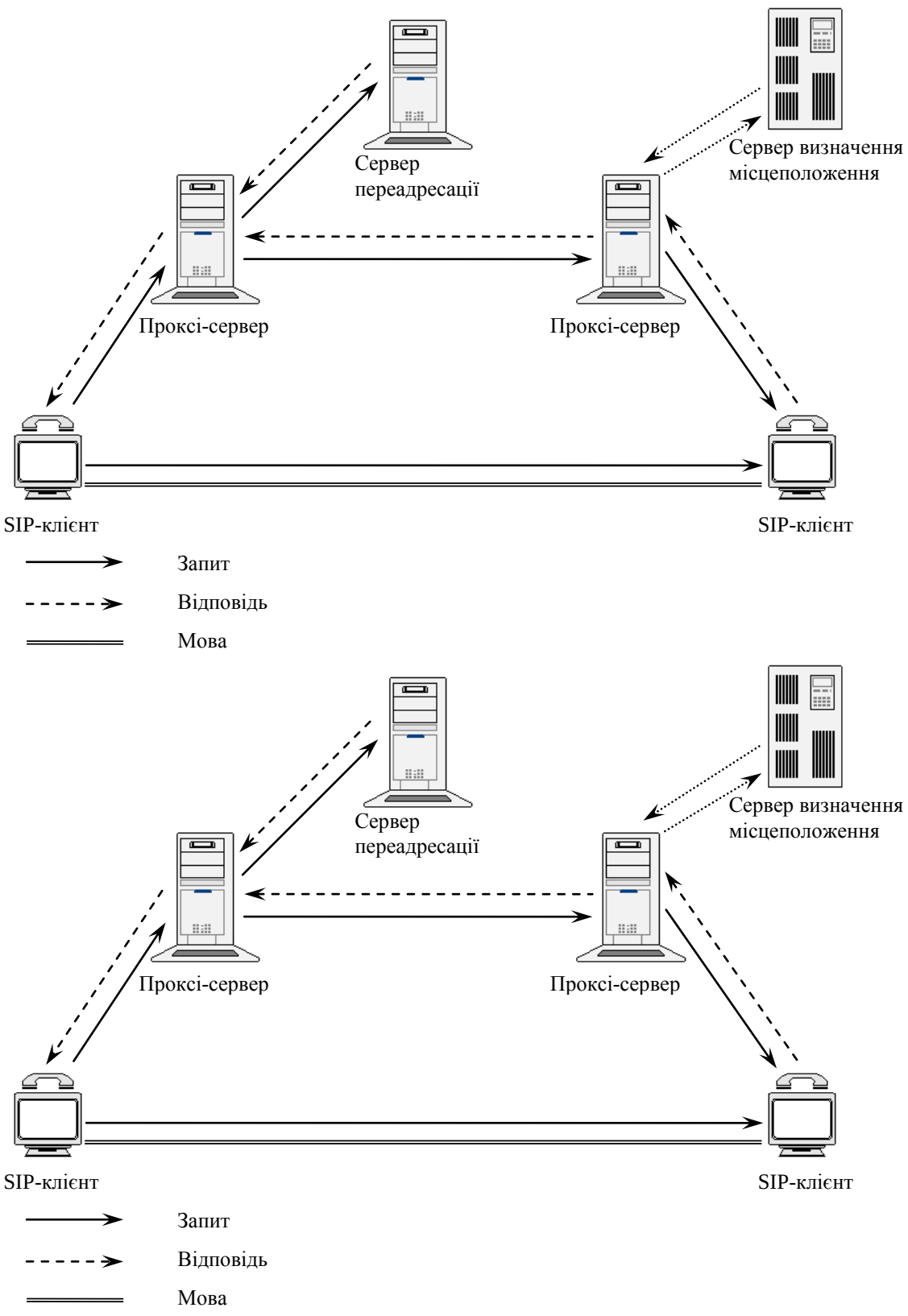
4.Архітектура мережі H.323.

5.Архітектура мережі на базі протоколу SIP.

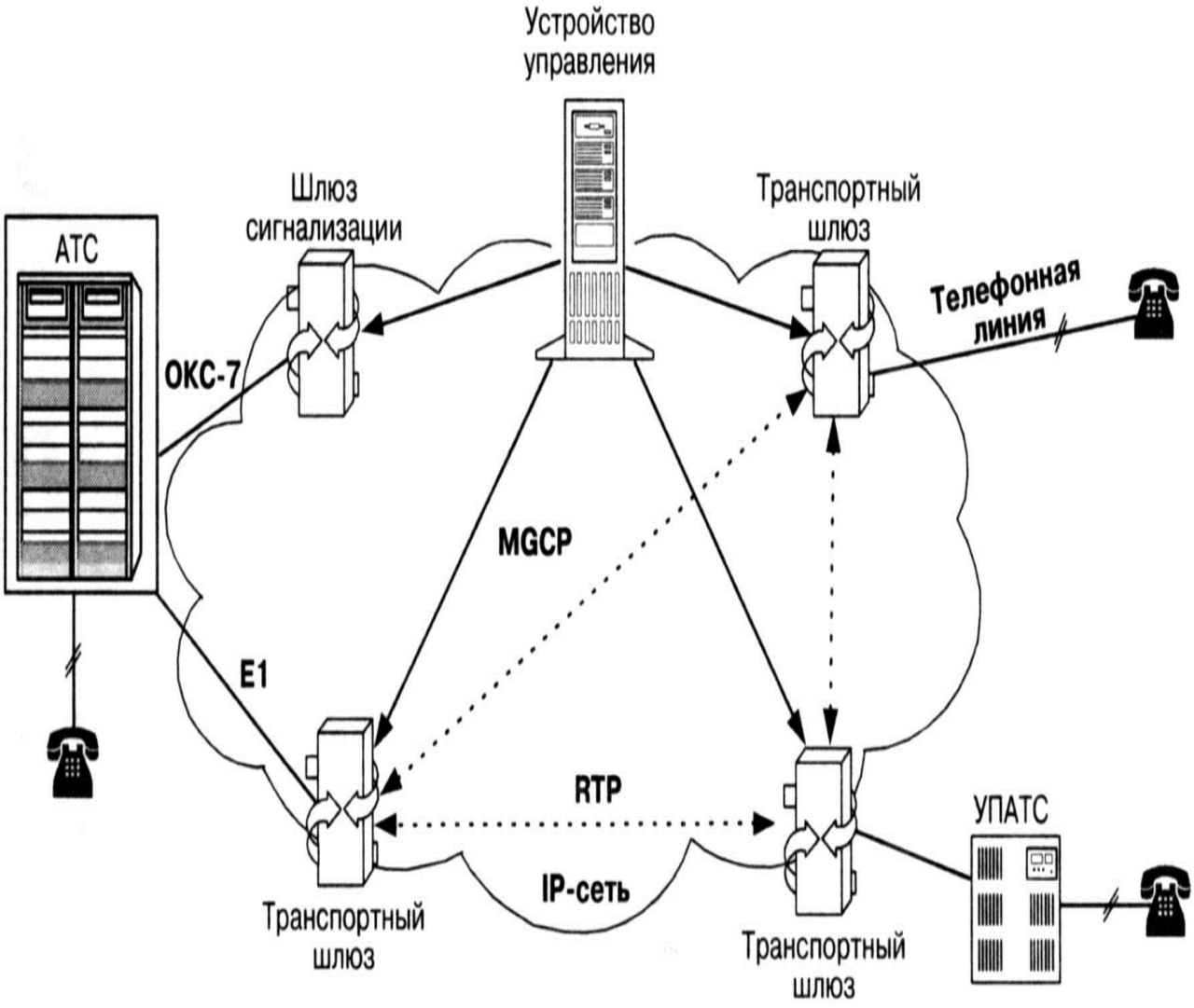

Пристрій
керування
конференціями
Термінал H.323
Термінал H.323
IP-мережа
Gatekeeper
Термінал H.323
Шлюз
ТМЗК
Шлюз
Мовний
термінал
Термінал
H.324
Термінал
H.320
Мовний
термінал



Архітектура мережі H.323



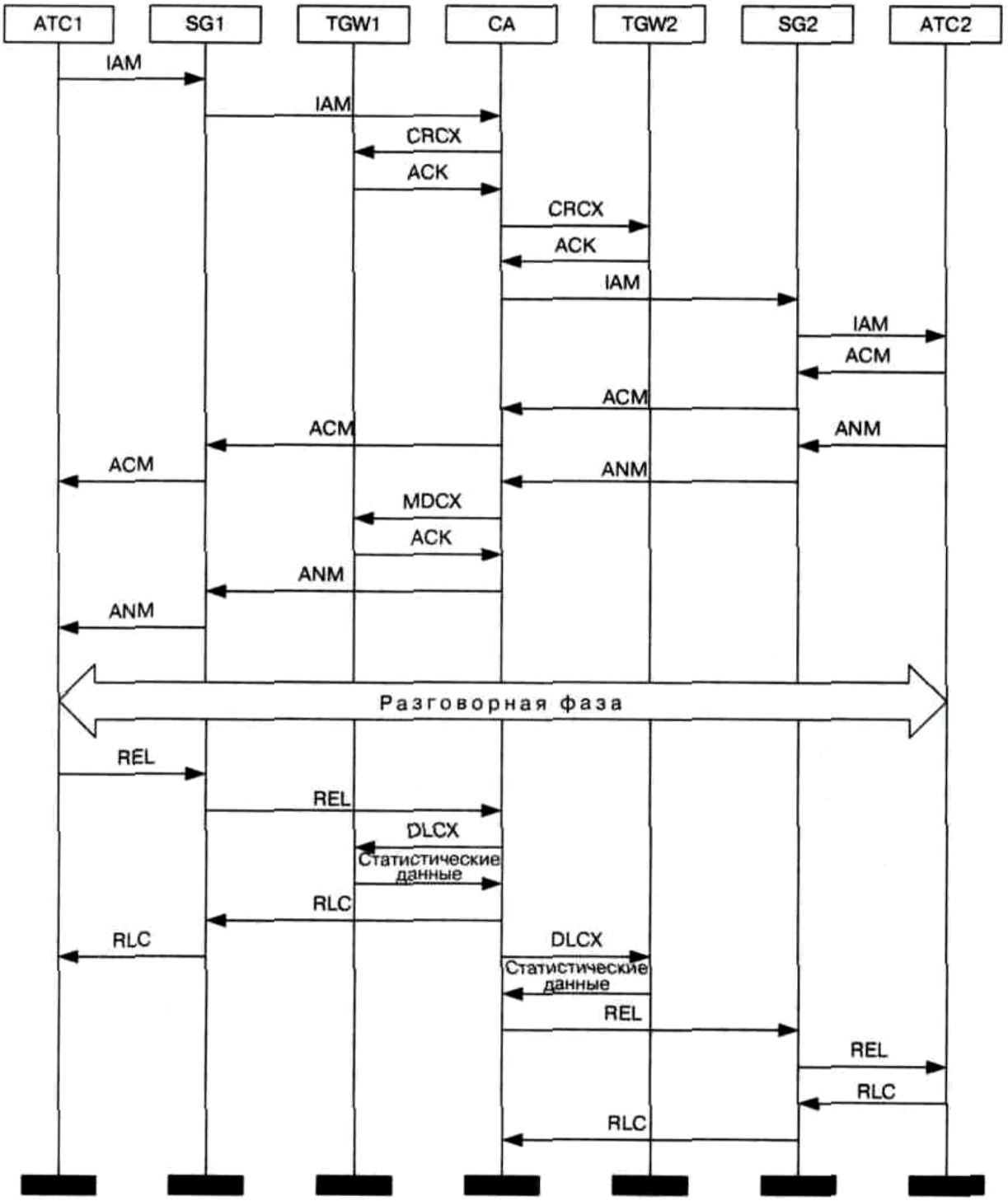
Архітектура мережі на базі протоколу SIP.



Архітектура мережі, що базується на протоколі MGCP.

Команди протоколу MGCP

Команда	Напрям передачі	Призначення
EndpointConfiguration (Конфігурація порту)	CA -> MG	Call Agent інструктує шлюз, яким чином йому потрібно обробляти одержувані мовні сигнали
CreateConnection (Створити з'єднання)	CA -> MG	Call Agent дає вказівку шлюзу створити з'єднання
ModifyConnection (Модифікувати з'єднання)	CA -> MG	Call Agent дає вказівку шлюзу змінити параметри існуючого з'єднання
DeleteConnection (Завершити з'єднання)	CA -> MG, MG -> CA	Call Agent і шлюзи завершують з'єднання
NotificationRequest (Запит повідомлення)	CA -> MG	Call Agent інструктує шлюз, які події необхідно виявляти.
Notify (Повідомити)	MG -> CA	Шлюз інформує Call Agent про те, що відбулося подія з числа тих, які були специфіковані в команді NotificationRequest
AuditEndpoint (Перевірити порт)	CA -> MG	Call Agent запрошує інформацію про який-небудь порт шлюзу
AuditConnection (Перевірити з'єднання)	MGC -> MG	Call Agent запрошує параметри з'єднання
ReStartlnProgress (Йде рестарт)	MG -> MGC	Шлюз інформує Call Agent про те, що один або декілька портів виводяться з робочого стану або повертаються в робочий стан



Приклад встановлення і руйнування з’єднання з використанням протоколу MGCP.

ВИСНОВКИ

Таким чином, в дипломній роботі викладені принципи побудови мереж IP-телефонії на підставі протоколу MGCP.

На основі проведеного вище порівняння можна зробити висновок, що для розгортання глобальних мереж IP-телефонії краще інших підходить протокол MGCP.

Розглянуто, що протокол SIP більше підходить для використання Internet-провайдерам, оскільки, в такому разі послуги IP-телефонії розглядаються лише як частина набору загальних послуг.

Відповідно, що оператори телефонного зв'язку, для яких послуги Internet не є першорядними, швидше за все, будуть орієнтуватися на протокол H.323, оскільки мережа, побудована на базі рекомендації H.323, представляється їм добре знайомою мережею ISDN, накладеною на IP-мережу.