ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ
ТЕЛЕКОМУНІКАЦІЙ

Пояснювальна записка

до магістерської кваліфікаційної роботи

на тему: **“ДОСЛІДЖЕННЯ МОЖЛИВОСТІ ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ НА ПІДСТАВІ ПРОТОКОЛУ H-323”**

Виконав: студент 6 курсу, групи ТСДМ-63
спеціальності
172 Телекомунікації та радіотехніка
(шифр і назва спеціальності)

Дударенко Р.В.
(прізвище та ініціали)

Керівник Антонюк М.І.
(прізвище та ініціали)

Рецензент
(прізвище та ініціали)

Нормоконтроль
(прізвище та ініціали)

Київ - 2019

ВСТУП

З моменту появи в березні 1995 року телефону VocalChat для підключення ПК до ПК від VocalTec в багатьох статтях в галузевій пресі часто стверджувалося, що найближчим часом телефонний трафік буде просто черговим додатком, що працює в Інтернеті. Такі висловлювання охоплюють багато технічних, нормативних та економічних деталей, які виключають можливість використання голосу в якості ще одного Інтернет-додатка. Ця теза є спробою забезпечити основу для розуміння того як технологія передачі голосу через Інтернет (VoIP) вплине на вибір регуляторних органів, не спекулюючи на природі нового регуляторного режиму.

З технічної точки зору Інтернет-протокол (IP), який не залежить від фізичного носія, забезпечує спосіб запуску VoIP як програми в дротових або бездротових мережах. Дротовою мережею може бути телефонна мережа загального користування (PSTN), кабельна, цифрова абонентська лінія (DSL) або Ethernet. Бездротовою мережею може бути мережа бездротового оператора, така як множинний доступ з кодовим поділом (CDMA), багаторазовий доступ з часовим розподілом (TDMA) або GSM, або приватні мережі, такі як WiFi, BlueTooth або WiMAX. Існує безліч різних структур, згідно з якими постачальник послуг може пропонувати послугу голосового зв'язку на основі VoIP. В одному крайньому випадку, можна запропонувати VoIP як додаток, який використовує будь-яку інфраструктуру, що пропонує Інтернет-зв’язок. У цьому випадку постачальник додатків не повинен володіти частинами інфраструктури. З іншого боку, може бути повна вертикальна інтеграція послуги, коли постачальник володіє інфраструктурою та всіма компонентами, необхідними для надання послуги. Отже, вибір структур визначає основні витрати, можливості та обмеження постачальника послуг. Це вимагає вивчення права власності на інфраструктуру при обговоренні варіантів регулювання різних сценаріїв, за яких послуги VoIP надаються споживачам.

Щодо регуляторної сторони, служба голосового зв’язку зазнала 100-річного регуляторного режиму. Інтернет, з іншого боку, звільнений від регулювання. Оскільки VoIP з'єднує два світи PSTN та Інтернет, питання для регуляторів поля-

гає в наступному: чи слід регулювати VoIP як загальнодоступний регламент, подібно до постачальника послуг зв'язку PSTN, залишати нерегульованим, як Інтернет, або регулюватися в рамках третього регуляторного режиму?. Тому актуальним є дослідження можливості побудови мереж IP-телефонії на підставі протоколу H.323 з метою управління перевантаженнями.

1 ОБҐРУНТУВАННЯ НЕОБХІДНОСТІ ВПРОВАДЖЕННЯ IP-ТЕЛЕФОНІЇ

1.1 Дослідження стеку протоколу IP-телефонії H.323

Голосовий зв’язок, що здійснюється за допомогою Інтернет-протоколу (IP) для транспортування, відомий як Протокол передачі голосу через Інтернет (VoIP). Традиційні телефонні мережі, відомі як телефонні комутаційні мережі загального користування (PSTN1), використовують комутацію каналів. У CircuitSwitching ресурси зарезервовані по всьому каналу зв'язку на час дзвінка. І навпаки, Інтернет-протокол (IP) використовує комутацію пакетів. У пакетному перемиканні інформація передається цифровим способом в один або кілька пакетів. Пакети знають своє місце призначення і можуть прибувати туди різними шляхами.

Впровадження VoIP вимагає ряду протоколів, від тих, що потрібні для сигналізації дзвінків для встановлення дзвінків та іншого, для передачі голосу в реальному часі через мережу, для маршрутизації, що забезпечує інформацію про якість послуг, резервування ресурсів, управління мережею, що знає QoS, і виставлення рахунків. Далі в цьому розділі ми розглянемо еволюцію кожного з цих протоколів, щоб зрозуміти, як вони відповідають сучасним популярним структурам.

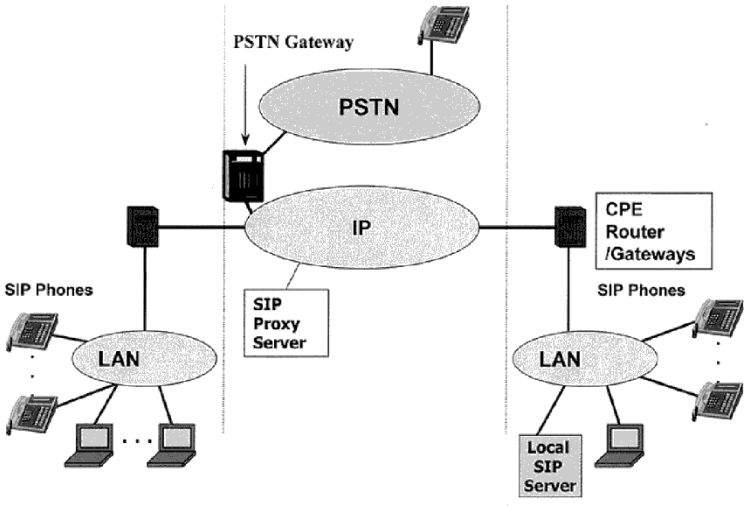

Рисунок 1. Наскрізний VoIP

Найчистіша реалізація VoIP використовує обладнання кінцевого споживача, яке підтримує IP, таке як IP-телефони або комп'ютер, і не покладається на стандартний телефонний комутатор. Малюнок 1 - спрощена схема IP-телефонної систе-

ми, підключеної до широкосмугової мережі IP. IP-телефони підключені до локальної мережі. Голосові дзвінки можна здійснювати локально через локальну мережу. IP-телефони включають кодеки, які оцифровують і кодують (а також декодують) мовлення. IP-телефони також пакують та депакетизують закодовану мову в IP-пакети. Дзвінки між різними сайтами можуть здійснюватися через IP-мережу широкого діапазону. Проксі-сервери виконують реєстрацію IP-телефонів та координують сигналізацію дзвінків, особливо між сайтами. Підключення до PSTN може здійснюватися через VoIP-шлюзи.

Оскільки голосовий зв'язок існує вже близько 100 років, існує дуже добре розвинена галузь, пов'язана з комутацією каналів PSTN. Є багато традиційних операторів з великою базою споживачів. У перші часи VoIP оператори мобільних телефонів вважали це загрозою для їхнього бізнесу та можливістю для постачальників мереж передачі даних, таких як Інтернет-провайдери. З часом діючі особи PSTN та нові учасники голосового зв'язку розглядають VoIP як можливість надання голосових послуг за значно зниженою вартістю [1]

Одним із способів зрозуміти розробку протоколів VoIP є сприйняття точки зору цих операторів PSTN, які намагаються зберегти та збільшити свою існуючу базу клієнтів, тоді як нові учасники голосового зв'язку з боку мережі передачі даних починають брати участь у всьому спектрі голосового зв'язку. Отже, специфічні структури та розробка протоколів для VoIP походять як із домену Міжнародного союзу телекомунікацій [2], [3]), який традиційно сприймається як організація зі стандартів, яка краще розуміє телефонію, так і з домену Цільовий групи інженерів Інтернету ([4] , [5]), який є основним органом, що відповідає за стандарти Інтернету та мереж передачі даних. Останнім часом спостерігається розробка протоколів у спільному домені [6]. Ці структури та протоколи були перевірені в телефонних мережах загального користування [7], в корпоративних телефонних мережах [8] та в Інтернеті [9]. У наступних підрозділах ми розглянемо еволюцію різних протоколів, необхідних для реалізації VoIP.

VoIP вимагає засобів для потенційних партнерів по спілкуванню, щоб знайти одне одного та сигналізувати іншій стороні про своє бажання спілкуватися. Ця

функціональність називається сигналізацією дзвінків. Потреба в функціонуванні сигналізації відрізняє Інтернет-телефонію від інших Інтернет-мультимедійних послуг, таких як послуги мовлення та медіа на замовлення.

VoIP, коли використовується для синхронного голосового або мультимедійного зв'язку між двома або більше сторонами, використовує сигналізацію, яка створює та керує дзвінками. Викликаний може визначити дзвінок як іменовану асоціацію між програмами, які явно налаштовані та зруйновані. Прикладами дзвінків є телефонні дзвінки з двома сторонами, мультимедійна конференція або багатокористувацька гра. Виклик може охоплювати ряд з'єднань, де з'єднання є логічним зв'язком між парою кінцевих систем у дзвінку. Наприклад, немостовий тристоронній аудіовиклик лише з трьома з'єднаннями матиме три з'єднання, створюючи повну сітку між учасниками. Медіапотік або сеанс - це потік одного типу медіа серед набору користувачів.

Цей потік може бути або одноадресним (у цьому випадку це між двома користувачами), або багатоадресним (більше двох користувачів). Медіа-сесія пов'язана з одним або кількома з'єднаннями. У наведеному вище прикладі тристороннього дзвінка, якщо мультимедіа поширюється за допомогою одноадресного передавання, на кожне з’єднання буде один аудіо-сеанс. Якщо аудіо розподіляється за допомогою багатоадресної передачі, буде один аудіо-сеанс, пов'язаний з усіма трьома з'єднаннями. Не обов'язково, щоб з викликами були пов'язані медіапотоків, але це, ймовірно, буде звичайним випадком.

Сигналізація Інтернет-телефонії може охоплювати ряд функцій: переклад імен та розташування користувача передбачає відображення назв різних рівнів абстракції, узгодження функцій дозволяє групі кінцевих систем домовитись про те, якими носіями обмінюватися, та їх відповідних параметрах, таких як кодування, дзвінок управління учасниками для того, щоб учасники запрошували інших на існуючий дзвінок або розривали з ними зв’язок, зміни функцій, що дозволяють коригувати склад медіа-сеансів під час дзвінка, або тому, що учасникам потрібна додаткова або обмежена функціональність, або через обмеження накладено або видалено додаванням або видаленням учасників дзвінка.

Існує кілька протоколів сигналізації VoIP-дзвінків. Ми обговоримо та порівняємо характеристики набору протоколів H.323, протоколу ініціювання сеансів (SIP), протоколу управління шлюзом медіа (MGCP) та Megaco / H.248. H.323 і SIP є одноранговими протоколами керування-сигналізації, тоді як MGCP та Megaco - протоколи управління-сигналізації ведучого-підлеглого. MGCP базується на моделі телефонної мережі PSTN. H.323 та Megaco призначені для проведення відеоконференцій, а також базової телефонії, але вони все ще засновані на парадигмі, орієнтованій на з'єднання, подібній до комутації каналів, незважаючи на те, що вони використовуються для систем пакетного зв'язку. Шлюзи H.323 мають більше функцій управління викликами, ніж медіа-шлюзи, що використовують MGCP, який передбачає, що більша частина інформації знаходиться в окремому контролері медіа-шлюзу. SIP був розроблений з нуля для IP-мереж і вміщує інтелектуальні термінали, зайняті не лише голосовими сеансами, але й іншими програмами.

Рекомендований ITU-T набір протоколів H.323 розвинувся зі стандарту відеотелефонії [10]. Коли першовідкривачі IP-телефонії розробляли власні продукти, промисловість закликала швидко розробити стандарт управління дзвінками VoIP, щоб користувачі та провайдери послуг мали можливість вибору постачальників та продуктів, які взаємодіють. Група активності передачі голосу за IP-адресами Міжнародного мультимедійного телекомунікаційного консорціуму (IMTC) рекомендувала H.323, який був розроблений для мультимедійних комунікацій через мережі пакетної передачі даних. Ці пакетні мережі можуть включати локальні мережі або глобальні мережі. IMTC дотримувався думки, що VoIP є особливим випадком IP-телефонії. Хоча не всі першовідкривачі VoIP погодились з тим, що відеотелефонія швидко стане популярною, набір протоколів H.323 став першим провідним стандартом для реалізації VoIP. Версії 2-4 стандарту включають модифікації, щоб зробити H.323 більш придатним для потреб VoIP.

Об'єкти H.323 можуть бути інтегровані в персональні комп'ютери або маршрутизатори або реалізовані в окремих пристроях. Для VoIP важливими об'єктами H.323 є термінали, шлюзи та гейткіпер H.323 (або контролер зони H.323). Шлюз H.323 забезпечує трансляцію протоколів та перекодування носія між кінце-

вою точкою H.323 та кінцевою точкою, яка не є H.323 (див. Малюнок 2). Наприклад, VoIP-шлюз забезпечує переклад форматів передачі та процедур сигналізації між телефонним комутованим каналом та пакетною мережею. Крім того, VoIP-шлюз може виконувати перекодування та стиснення мови, і він, як правило, здатний генерувати та виявляти двотональні багаточастотні сигнали (DTMF) (тобто тональний сигнал).

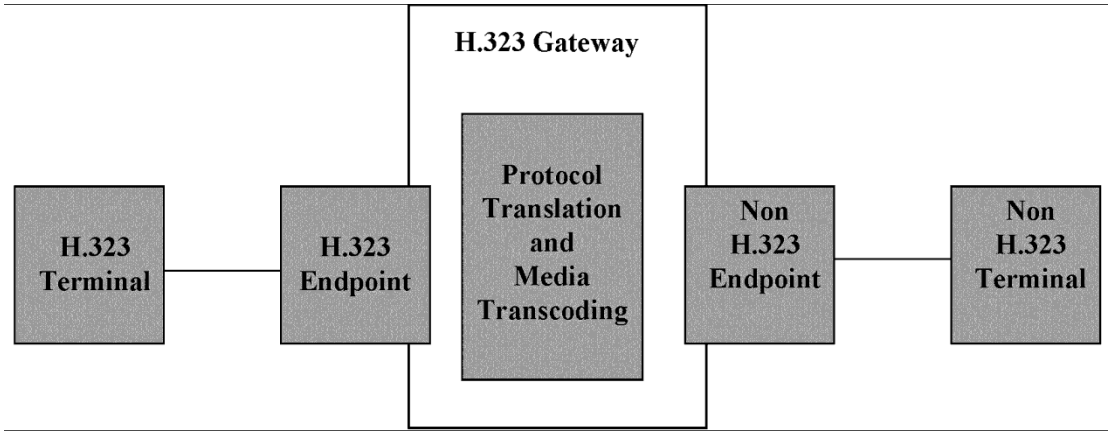

Рисунок 2 Шлюз H.323

Елементи терміналу VoIP H.323 включають наступне:

- Блок управління системою забезпечує сигналізацію для належної роботи терміналу H.323, який забезпечує управління викликами за допомогою H.225.0 та H.245 (описано нижче).
- Рівень H.225.0 форматує передані аудіопотоки і потоки управління в повідомлення, витягує аудіопотоки з повідомлень, отриманих від мережевого інтерфейсу, і виконує логічне кадрування, порядкову нумерацію, виявлення помилок і виправлення помилок, якщо це необхідно.
- Аудіокодек перекодує, а також може стискати мову . Гейткіпер H.323 виконує функції контролю доступу та функції перекладу адрес. Кілька гейткіпер H.323 можуть спілкуватися між собою для координації своїх служб контролю.

Мережі з VoIP-шлюзами повинні (але не зобов’язані) мати гейткіпер H.323

для перетворення вхідних адрес E.164 у транспортні адреси (наприклад, IP-адреса та номер порту). Гейткіпер H.323 логічно відокремлений від інших сутностей H.323, але фізично він може співіснувати з терміналом, шлюзом або проксі H.323. Перебуваючи у мережі VoIP, гейткіпер H.323 забезпечує наступні функції:

• Переклад адрес - гейткіпер H.323 переводить псевдоніми (наприклад, телефонні номери E.164) у транспортні адреси, використовуючи таблицю перекладів, яка оновлюється за допомогою реєстраційних повідомлень та інших засобів.

• Контроль за допуском - гейткіпер H.323 авторизує доступ до мережі, використовуючи повідомлення H.225. Критерії прийому можуть включати авторизацію дзвінків, пропускну здатність або інші правила.

• Контроль пропускної здатності - гейткіпер H.323 контролює, яку смугу пропускання може використовувати термінал.

• Управління зонами - термінал може реєструватись лише з одним гейткіпером H.323 одночасно. Гейткіпер H.323 забезпечує вищезазначені функції для терміналів та шлюзів, які зареєструвались у ньому.

• Участь у сигналізації управління дзвінками необов’язкова.

• Послуги каталогів є необов’язковими.

Коли кінцева точка (наприклад, телефон) підключена до мережі, канал реєстрації, прийому та стану (RAS) передає повідомлення, що використовуються в процесах реєстрації кінцевих точок гейткіпера H.323, які пов'язують псевдонім кінцевої точки (наприклад, телефонний номер E.1643) з її TCP / IP-адреса та номер порту, які будуть використовуватися для сигналізації дзвінків. Канал RAS також використовується для передачі повідомлень про допуск, зміну пропускної здатності, стан та відключення повідомлень між кінцевою точкою та її гейткіпером H.323. H.225.0 рекомендує тайм-аути та кількість повторних спроб для повідомлень RAS, оскільки вони передаються на ненадійному каналі протоколу користувацьких дейтаграм (UDP) .

Канал сигналізації дзвінків передає повідомлення управління викликами H.225.0 за допомогою TCP, що робить його надійним каналом. Кінцеві точки

H.323 і гейткіпери H.323 використовують повідомлення Q.931 (з TCP) для сигналізації дзвінків. У мережах, де немає гейткіпера H.323, кінцеві точки надсилають повідомлення сигналізації виклику безпосередньо до викликаної кінцевої точки, використовуючи транспортні адреси сигналізації дзвінків. Якщо в мережі є гейткіпер H.323, виклична кінцева точка надсилає початкове повідомлення про прийняття гейткіпера H.323, використовуючи транспортну адресу RAS каналу гейткіпер H.323. При початковому обміні повідомленнями про допуск гейткіпера H.323 повідомляє вихідній кінцевій точці, чи слід надсилати повідомлення сигналізації виклику безпосередньо в іншу кінцеву точку, чи направляти їх через гейткіпер H.323. Сигналізація дзвінків може бути направлена двома шляхами: пряма сигналізація виклику кінцевої точки та сигналізація дзвінків маршрутизатора.

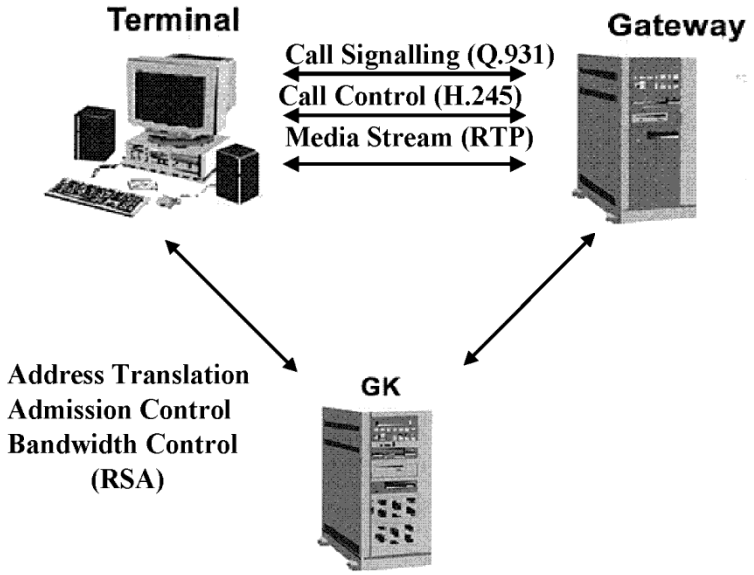

Рисунок 3 Пряма сигналізація виклику кінцевої точки

На рисунку 3 показано пряму сигналізацію виклику кінцевої точки, яка надсилає повідомлення сигналізації виклику безпосередньо між кінцевими точками або шлюзами. При прямій сигналізації виклику кінцевої точки гейткіпер H.323 бере участь у прийомі викликів, але безпосередньо не знає про зв'язки. Через обмежену участь один гейткіпер H.323 може обробляти велику кількість дзвінків, але гейткіпер H.323 має обмежені можливості виконувати функції управління послугами. Гейткіпер H.323 не може визначити швидкість завершення виклику, і, якщо він повинен виконувати запис детальної інформації про виклик, він повинен

залежати від кінцевих точок інформації про тривалість дзвінка.

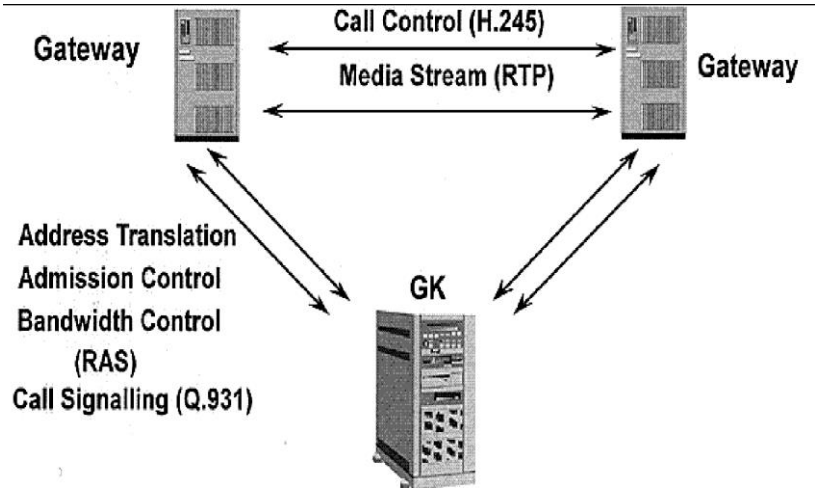

Рисунок 4 Сигналізація виклику маршрутизатора (Q.931)

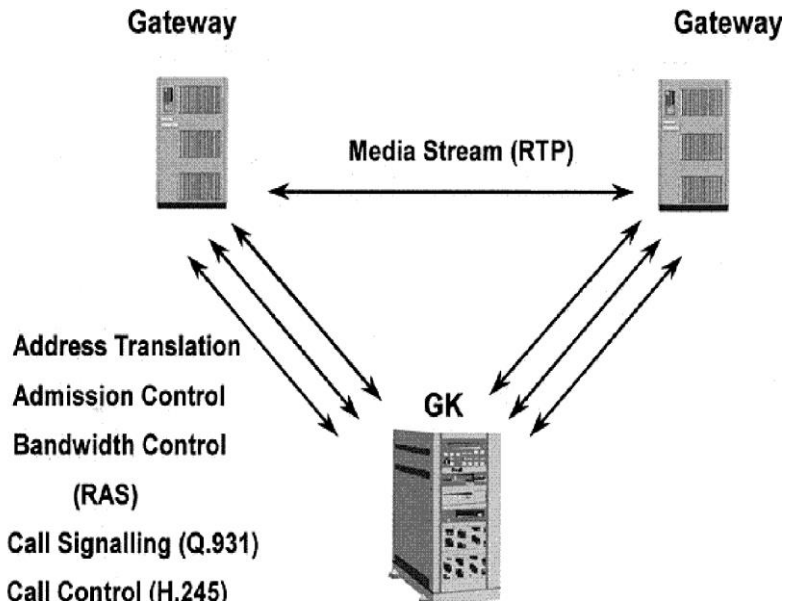

Рисунок 5 Сигналізація виклику маршрутизатора (Q.931 / H.245)

На малюнках 4 і 5 показана маршрутизована сигналізація викликів гейткіпера H.323, яка направляє повідомлення сигналізації викликів від однієї кінцевої точки через гейткіпер H.323 до іншої кінцевої точки. Метод сигналізації виклику маршрутизатора призводить до більшого навантаження на гейткіпера H.323, оскільки він повинен обробляти повідомлення Q.931. Гейткіпер H.323може закрити канал сигналізації дзвінка після завершення налаштування дзвінка. Однак, якщо гейткіпер H.323 залишається залученим у дзвінок, наприклад, для створення записів викликів або для підтримки додаткових послуг, він буде тримати канал відк-

ритим протягом усього часу дзвінка.

Канал управління H.245 передає наскрізні контрольні повідомлення H.245, що регулюють роботу об'єктів H.323 (хост H.323, шлюз H.323 або воротар H.323). Ключовою функцією каналу управління H.245 є обмін можливостями. Інші функції H.245 включають відкриття та закриття логічних каналів, повідомлення про управління потоком, запити щодо переваги режиму та загальні команди та індикації. Кінцева точка встановлює канал управління H.245 для кожного виклику, в якому бере участь кінцева точка. Цей логічний канал управління H.323 відкритий протягом усього періоду дзвінка. Щоб відповідати Рекомендації H.245, кінцеві точки H.323 повинні підтримувати синтаксис, семантику та процедури таких сутностей протоколу:

- визначення ведучого / веденого;
- обмін можливостями;
- логічна сигналізація каналу;
- двонаправлена сигналізація логічного каналу;
- сигналізація закритого логічного каналу;
- запит режиму;
- визначення затримки прийому-передачі;
- сигналізація циклу технічного обслуговування.

Як приклад того, як використовується H.245, обговоримо, як він вміщує просту телефонну сигналізацію.

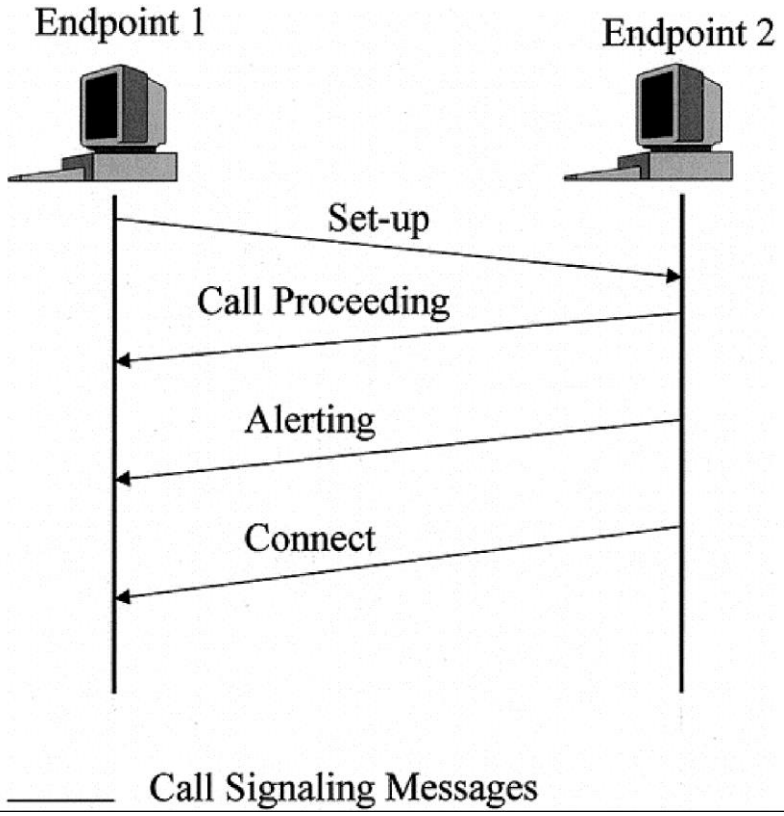

Рисунок 6. Основна настройка виклику з гейткіпером H.323.

На рисунку 6 показано основну сигналізацію налаштування виклику для випадку, коли жодна кінцева точка не зареєстрована у воротаря. Кінцева точка виклику (кінцева точка 1) надсилає повідомлення про налаштування (1) до відомого ідентифікатора TSAP каналу сигналізації виклику (порт TCP # 1720) кінцевої точки 2.

Кінцева точка 2 відповідає викликом (2), попередженням (3) і, нарешті, повідомленням про підключення (4), що містить транспортну адресу транспортного каналу управління H.245 для використання в сигналізації H.245.

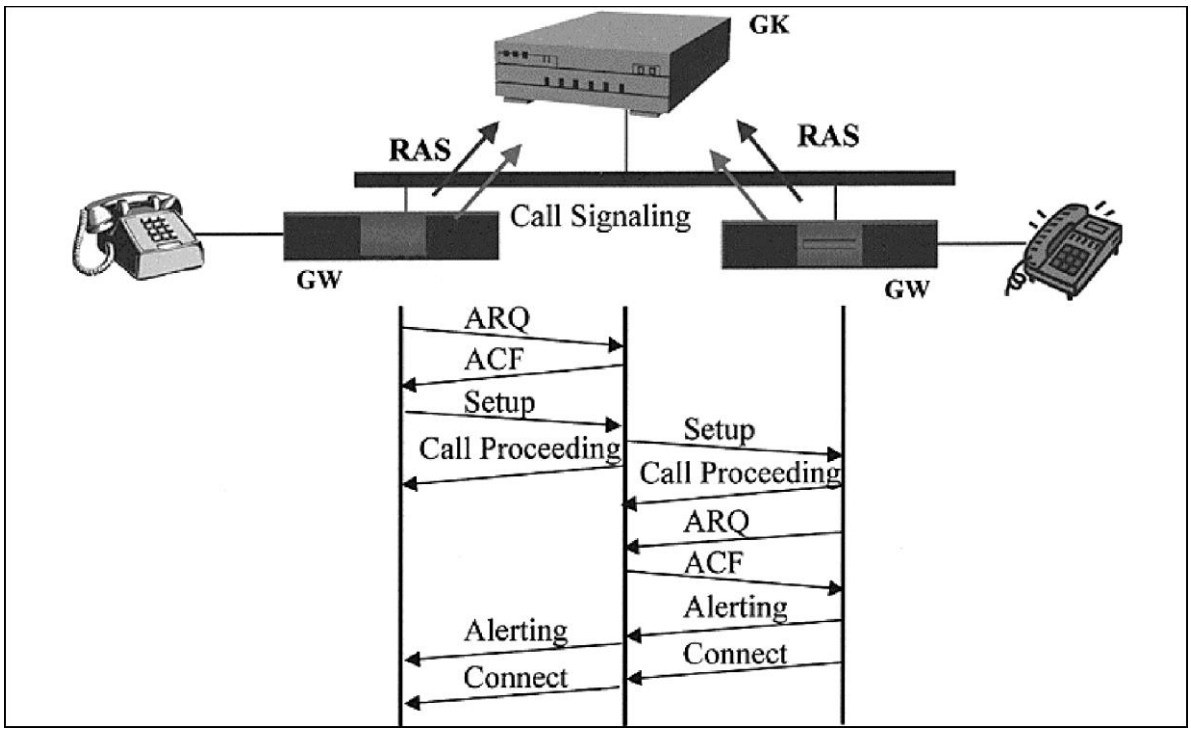

Рисунок 7. Базова настройка дзвінків із сигналізацією дзвінків, що перенаправляють гейткіпера H.323.

На рисунку 7 показано базову настройку сигналізації дзвінків, що перенаправляє гейткіпер H.323. Спочатку шлюз-джерело надсилає запит на допуск (ARQ) гейткіперу H.323, який відповідає підтвердженням про допуск (ACF). Потім налаштування продовжується, як зазначено.

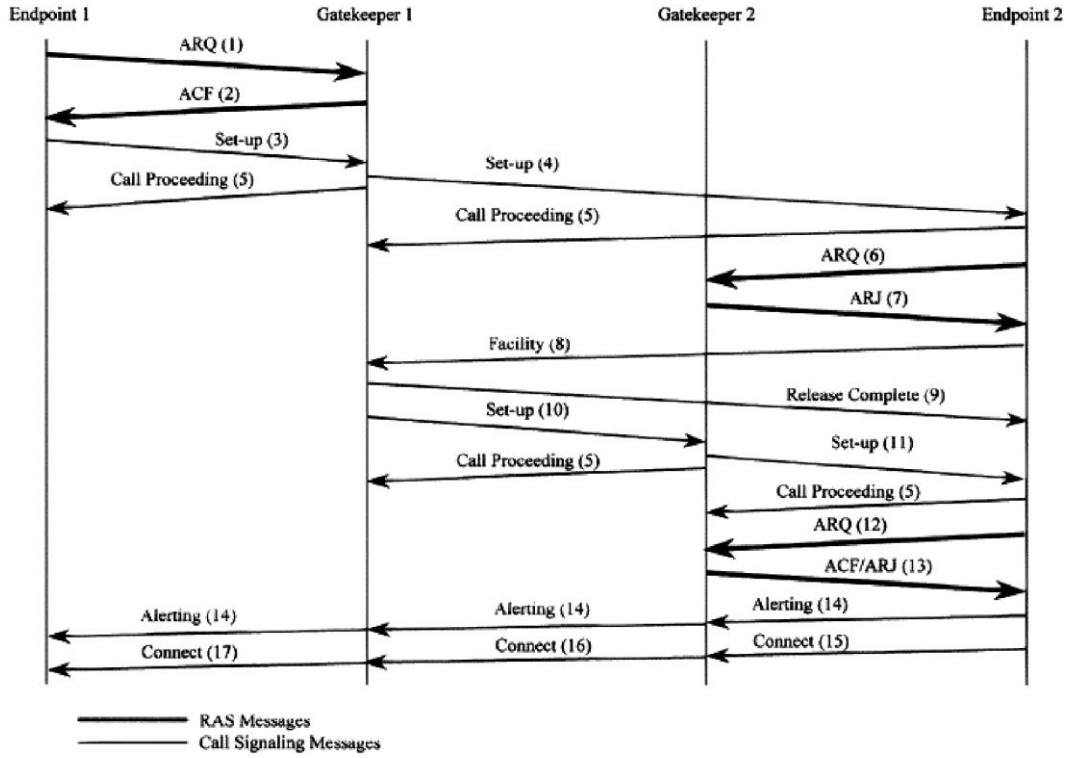

Рисунок 8 Сигналізація виклику маршрутизатора за участю двох гейткіперів H.323.

На рисунку 8 показано налаштування дзвінків, де обидві кінцеві точки реєструються в окремих гейткіперах H.323, і обидві використовують сигналізацію дзвінків, спрямовану на гейткіпера H.323. Зверніть увагу, що на цих діаграмах явно не показано встановлення TCP-з'єднань між кінцевими точками та сторожами. Перша частина налаштування виклику схожа на випадок з одним гейткіпером H.323, показаний на рисунку 7. Коли повідомлення про встановлення виклику досягає кінцевої точки 2, воно ініціює обмін ARQ (6) / ACF (7) з воротарем 2. Припускаючи, що виклик прийнятний , гейткіпер H.323 2 надсилає власну адресу сигналізації дзвінка у повідомленні про відхилення ARJ (7) (замість ACF) із кодом причини, що командує кінцевій точці, щоб направити на неї сигналізацію виклику. Решта схеми сама собою пояснюється.

Як видно з рисунка 8, сигналізація дзвінків може включати багато повідомлень, що передаються вперед і назад серед об'єктів H.323.

2 ПРИНЦИП ПОБУДОВИ МЕРЕЖ НА ПІДСТАВІ ПРОТОКОЛУ SIP-Т ПРОТОКОЛ ІНІЦІЮВАННЯ СЕСІЇ (SIP)

SIP [5] - це протокол управління (або сигналізації), подібний до HTTP. Це протокол, який може налаштувати та зруйнувати будь-який тип сеансу. Контроль викликів SIP використовує протокол опису сеансу (SDP) [11] для опису деталей виклику (тобто аудіо, відео, спільного додатка, типу кодека, розміру пакетів тощо). SIP використовує універсальний локатор ресурсів (URI) 6 для ідентифікації логічного пункту призначення, а не IP-адреси. Адреса може бути псевдонімом, адресою електронної пошти (наприклад, sip: chintanv@mit.edu) або номером телефону. На додаток до телефонного дзвінка, SIP може сповіщати користувачів про події, такі як "Я в мережі", "людина зайшла в кімнату" або "електронна пошта надійшла". SIP також можна використовувати для надсилання миттєвих текстових повідомлень.

SIP використовує модель клієнт-сервер. Клієнти відправляють запити SIP, тоді як сервери приймають запити SIP, виконують запитувані методи та відповідають. Специфікація SIP визначає шість методів запиту:

• REGISTER дозволяє або користувачеві, або третій стороні зареєструвати контактну інформацію на SIP-сервері.

• INVITE ініціює послідовність сигналізації дзвінків.

• Налаштування сеансу підтримки ACK та CANCEL.

• BYE завершує сеанс.

• OPTIONS запитує сервер про його можливості.

Нижче перелічено деякі важливі функціональні сутності SIP.

• Агент користувача виконує функції як клієнта агента користувача, який ініціює запит SIP, так і сервера агента користувача, який зв'язується з користувачем при отриманні запиту SIP і повертає відповідь від імені користувача.

• Проксі-сервер SIP виступає як клієнтом SIP, так і сервером SIP при надсиланні запитів SIP від імені інших клієнтів SIP. Проксі-сервер SIP може бути як з відстеженням стану, так і без нього. Проксі-сервер повинен мати відстеження ста-

ну, щоб підтримувати TCP або різні служби. Однак проксі-сервер без збереження стану краще масштабується (підтримує більш високі обсяги викликів).

• Реєстратор - це SIP-сервер, який приймає, аутентифікує та приймає запити REGISTER від клієнтів SIP. Він може бути розміщений за допомогою проксі-сервера SIP.

• Сервер локації зберігає інформацію про користувачів у базі даних і допомагає визначити, куди (на яку IP-адресу) надіслати запит. Він також може бути розміщений за допомогою проксі-сервера SIP.

• Сервер переадресації не має стану. Він відповідає на запит SIP адресою, за якою ініціатор запиту може зв'язатись безпосередньо з бажаним об'єктом. Він не приймає дзвінки та не ініціює власні запити.

SIP визначає логічні сутності, які можуть бути реалізовані окремо або разом в одному продукті.

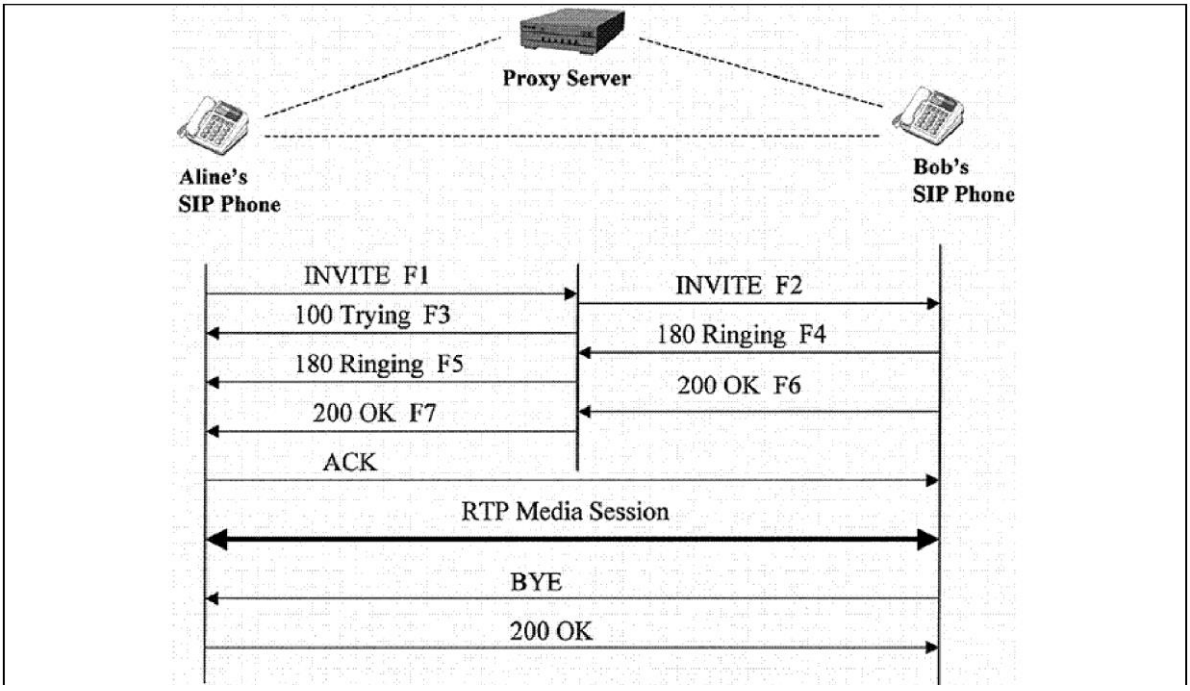

Рисунок 9 Налаштування сеансу SIP з одним проксі-сервером.

Ми використовуємо два простих приклади для пояснення основних операцій SIP. Перший приклад використовує єдиний проксі-сервер, як це було б вірогідно для IP-телефонії на базі SIP в межах однієї корпоративної будівлі або кампусу.

Аліна дзвонить Бобу, щоб задати питання про SIP. Аліна і Боб працюють в одному корпоративному кампусі будівель, що обслуговуються одним і тим же проксі-сервером SIP. Оскільки Аліна і Боб не телефонують один одному регулярно, SIP-телефон Аліни не має IP-адреси SIP-телефону Боба. Тому сигналізація SIP проходить через проксі-сервер SIP. Аліна набирає приватний номер Боба (555-6666). Її SIP-телефон перетворює цей приватний номер у відповідний SIP-URI (sip: 555-6666@nice.com) і надсилає ЗАПРОШЕННЯ на проксі-сервер SIP. Рисунок 9 показує обмін повідомленнями SIP для цього прикладу.

SIP використовує модель транзакції запиту / відповіді, подібну до HTTP. Кожна транзакція починається із запиту (простим текстом), який викликає серверну функцію ("метод"), і закінчується відповіддю. У нашому прикладі SIP-телефон Аліни починає транзакцію, надіславши

Запит INVITE на SIP URI Боба (sip: 555-6666@nice.com). Запит INVITE містить поля заголовка, які надають інформацію, що використовується при обробці повідомлення, таку як ідентифікатор виклику, адреса призначення, адреса відправника та запитаний тип сеансу. Ось ЗАПРОШЕННЯ Аліни (повідомлення F1 на малюнку 9):

• ЗАПРОСИТИ sip: bob@nice.com SIP / 3.0

• Через: SIP / 3.0 / UDP 192.2.4.4:5060

• Кому: Боб <'sip: 555-6666@nice.com>

• Від: Aline .silly555-1234 @ nice.com; tag = 203 941 885

• Call-ID: b95c5d87f7721@192.2.4.4

• Cseq: 26, 563 897 INVITE

• Контакт: sip: 555-1234@192.2.4.4

• Тип вмісту: application / sdp.

• Довжина контакту: 142

(SDP Аліни не показаний)

Перший рядок дає назву методу (INVITE). Ми опишемо поля заголовка у наступних рядках прикладу повідомлення ЗАПРОШУВАННЯ, яке містить мінімально необхідний набір:

• *Через* містить IP-адресу (192.2.4.4), номер порту (5060) та транспортний протокол (UDP), які Аліна хоче, щоб Боб використовував у своїй відповіді.

• *Кому* містить відображуване ім'я (Bob) та URI SIP (sip: 555-6666@nice.com), на який було надіслано цей запит.

• *Від* містить коротке ім'я (Aline) і SIP-URI (SIP: 555-1234@nice.com), які ідентифікують запит відправнику.

• *Call-ID* містить глобальний унікальний ідентифікатор цього дзвінка.

• Ці три рядки (Кому, Від і Ідентифікатор виклику) визначають взаємозв'язок між одноранговою мережею SIP.

SIP-телефон Аліни та SIP-телефон Боба, який іноді називають "діалоговим вікном".

Послідовність команд (Cseq) містить ціле число та ім'я методу. Аліна

SIP-телефон збільшує номер Cseq(*це заголовок, що допомагає ідентифікувати транзакцію в рамках діалогу*) для кожного нового запиту.

Контакт містить ім’я користувача та IP-адресу Аліни у вигляді SIP-URI. Поки заголовок *Через* повідомляє SIP-телефону Боба, куди надіслати відповідь, заголовок *Контакт* повідомляє і проксі-серверу, і SIP-телефону Боба, куди надсилати майбутні запити на це діалогове вікно.

Тип вмісту описує тіло повідомлення.

Довжина контакту дає довжину (в октетах) тіла повідомлення.

Тіло SIP-повідомлення містить опис сеансу, такий як тип носія, тип кодека, розмір пакета тощо, у форматі, встановленому (зазвичай) SDP. Спосіб передачі повідомлення SIP повідомлення SDP аналогічний способу передачі повідомлення HTTP веб-сторінки.

Оскільки SIP-телефон Аліни не знає IP-адреси Боба, повідомлення INVITE спочатку надходить на проксі-сервер SIP. Коли він отримує запит INVITE, проксі-сервер відправляє відповідь 100 Спроба назад на SIP-телефон Аліни, вказуючи, що проксі намагається направити INVITE на SIP-телефон Боба. Як правило, SIP-відповіді мають числовий тризначний код, за яким слідує описова фраза. Ця відповідь (Повідомлення F3 на рисунку 9) містить те саме значення, що надходить,

від ідентифікатора виклику та заголовка Cseq, як і повідомлення ЗАПРОШУВАТИ, і SIP-телефон Аліни може співвіднести цю відповідь із надісланим. Проксі-сервер додає ще один заголовок *Через (Via)* із власною IP-адресою до INVITE та пересилає його (Повідомлення F2 на малюнку 9) на SIP-телефон Боба.

Коли SIP-телефон Боба отримує ЗАПРОШЕННЯ, він попереджає (дзвонить) Бобу, щоб він міг вирішити, чи відповідати. Оскільки ім'я Аліни є в заголовку До, SIP-телефон Боба може відображати ім'я Аліни. SIP-телефон Боба надсилає відповідь 180 дзвінка через проксі-сервер назад на SIP-телефон Аліни. Проксі використовує заголовок *Через (Via)*, щоб визначити, куди надсилати відповідь, і видаляє власну адресу зверху. Коли SIP-телефон Аліни отримує відповідь 180 дзвінка, це вказує на дзвінок, відображаючи повідомлення на дисплеї SIP-телефону або звуковим сигналом зворотного дзвінка.

Коли Боб натискає кнопку гучного зв'язку, його SIP-телефон надсилає відповідь 200 OK, щоб вказати, що він відповів на дзвінок. Тіло повідомлення 200 OK містить опис засобів масової інформації SDP типу сеансу, який може встановити SIP-телефон Боба під час цього дзвінка. Таким чином, відбувається двосторонній обмін повідомленнями SDP, обговорюючи можливості, які будуть використані для дзвінка. SIP-телефон Аліни надсилає ACK безпосередньо на SIP-телефон Боба (він не проходить через проксі-сервер без збереження стану), і Аліна може спілкуватися з Бобом через медіасесію RTP. Зверніть увагу, що фактичні голосові пакети маршрутизуються безпосередньо з одного SIP-телефону на інший, і їх заголовки не мають інформації про SIP-повідомлення або проксі-сервери, які налаштовують сеанс медіа RTP.

У цьому прикладі Боб не може відповісти на питання Аліни, але пропонує їй зателефонувати Генрі в Даллас. Генрі - експерт по SIP, але він працює в іншій компанії global.com. У Боба є адреса електронної пошти Генрі, але не його номер телефону. Коли Боб прощається і натискає кнопку, його SIP-телефон відправляє «BYE» прямо на SIP-телефон Аліни. SIP-телефон Аліни відповідає повідомленням 200 OK, що завершує виклик, включаючи медіа-сеанс RTP.

Тепер Аліна дзвонить Генрі (див. Малюнок 10), використовуючи портатив-

ний комп'ютер, підключений до її SIP-телефону. Аліна вводить адресу електронної пошти Генрі і натискає кнопку, щоб встановити телефонний дзвінок SIP. SIP-телефон Аліні надсилає ЗАПРОШЕННЯ на адресу SIP URI Генрі, яке базується на його електронній адресі (henry@global.com). Оскільки проксі-сервер Nice.com не знає, як перенаправити виклик Генрі, він використовує службу імен доменів (DNS) для пошуку SIP-сервера global.com.

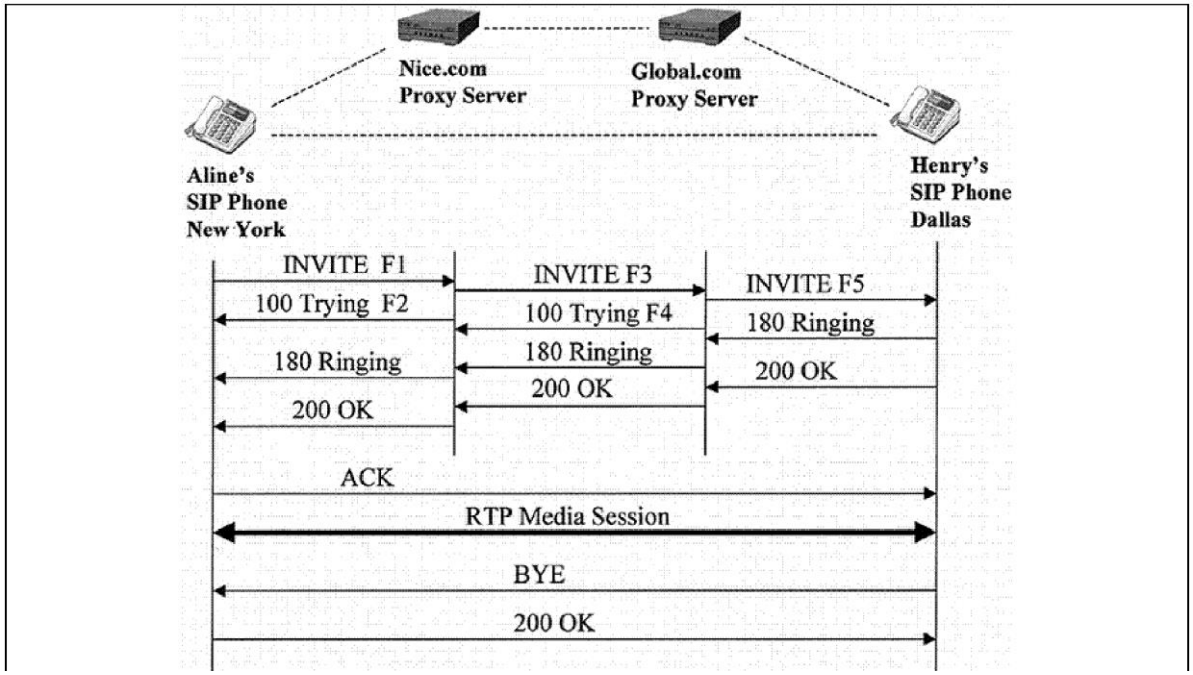

Рисунок 10. Налаштування SIP-дзвінка з двома проксі-серверами.

Насправді, що потрібно серверу Nice.com, це перелік наступних переходів, які можна використовувати для доступу до сервера global.com. Наступний перехід визначається поєднанням IP-адреси, порту та транспортного протоколу. Специфікація SIP дає алгоритм визначення впорядкованого списку наступних переходів.

ЗАПРОШЕННЯ Аліни (повідомлення F1 на малюнку 10) схоже на те, що вона надіслала Бобу:

• ЗАПРОСИТИ sip: henry@global.com SIP / 3/0

• Через: SIP / 3.0 / UDP 192.2.4.4:5060

• Кому: Генрі <sip: henry@global.com

• Від: Aline <sip: alme@nice.com>; тег = 9 817 514 140

• Call-ID: z73a3b65d55609@192.2.4.4

• Cseq: 704 452 ЗАПРОШУЙТЕ

• Контакт: <: sip: alme@192.2.4.4>

• Тип вмісту: application / sdp тощо.

Зверніть увагу, що в цьому повідомленні INVITE ідентифікатори SIP URI базуються на адресах електронної пошти, а не на номерах телефонів. Потік повідомлень подібний до налаштування виклику Бобу, за винятком того, що повідомлення SIP тепер проходять через проксі-сервер global.com, а також проксі-сервер nice.com, як показано на малюнку 10.

SIP дозволяє проксі-серверам приймати складні рішення щодо того, куди відправити ЗАПРОШЕННЯ. У цьому прикладі Генрі міг подорожувати і його дзвінки переадресовували в офіс компанії у Вашингтоні, округ Колумбія. Проксі-сервер може одночасно відправити ЗАПРОШЕННЯ у кілька місць, щоб дзвінок міг одночасно перенаправлятися на сервер голосової пошти Генрі в Далласі та його гостьовий офіс у Вашингтоні. Якщо Генрі відповість на дзвінок у Вашингтоні, сеанс із сервером голосової пошти може бути припинено.

Запит INVITE може містити інформацію, яка буде використана проксі-сервером призначення для визначення набору цільових дзвінків. Наприклад, цільові набори можуть бути побудовані на основі часу доби, інтерфейсу, на який надійшов запит, відмови попередніх запитів або поточного рівня використання розподільника викликів. Аліна може запрограмувати свій SIP-телефон запитувати послугу подальшого обслуговування лише в місцях бізнесу. З іншого боку, Генрі може запрограмувати свій SIP-сервер для переадресації дзвінків на свій мобільний телефон, але лише список із привілейованим доступом (сім'я та начальник?) Міг би переадресовувати дзвінки до нього додому.

SIP сприяє мобільності, оскільки одна і та ж особа може користуватися різними терміналами з однаковою адресою та однаковими послугами. SIP обіцяє бути використаний багатьма програмістами для розробки нових послуг. Багато з цих нових послуг можуть бути запропоновані в загальнодоступному Інтернеті.

Таблиця 1. Види послуг, які можна запропонувати за допомогою SIP

Послуги, подібні PSTN	Нові послуги
Ідентифікатор абонента	Інтернет / голосова інтеграція
PBX- як функції	Програмовані послуги
Переадресація викликів	Маршрутизація з декількома пунктами призначення
Переадресація дзвінка	Присутність
AIN- як функції	Миттєві повідомлення
Безкоштовний виклик	Мультимедіа
Знайди мене / слідуй за мною	Повідомлення про подію
Конференц-дзвінки	Виклик абонента та телефонні преференції
	Єдина система обміну повідомленнями

SIP дозволяє легко додавати нові послуги третіми сторонами. Корпорація Майкрософт включила стек SIP в Windows XP, останню операційну систему для настільних ПК, і має певний графік випуску нового API-сервера .NET, який стане наступником сервера Windows 2000. Оскільки SIP буде підтримувати інтелектуальні пристрої, які потребують незначної підтримки додатків з мережі, а також не інтелектуальні пристрої, які потребують великої підтримки з боку мережі, ми маємо можливість, аналогічну переходу від спільних комп'ютерів до персональних комп'ютерів. У 1960-70-х роках ми використовували німі термінали для доступу до програм на основному комп'ютері, яким користувались багато сотень користувачів. Починаючи з 1980-х років, ми почали використовувати складні програми на ПК, але ми також змогли використовувати ПК як комунікаційний термінал для отримання доступу до додатків та баз даних на спільних комп'ютерах (серверах) у мережі. Хости SIP з різним ступенем витонченості виконуватимуть деякі функції локально, дозволяючи нам отримувати доступ до програм у мережі. SIP у цьому

відношенні відрізняється від H.323. Хоча модель H.323 вимагає взаємодії додатків за допомогою управління викликами, користувачі SIP можуть взаємодіяти безпосередньо з програмами.

SIP можна використовувати для створення нових послуг на додаток до тиражування традиційних телефонних послуг. Присутність і обмін миттєвими повідомленнями є прикладом нового типу послуги, яка може використовувати SIP. Існує кілька популярних систем обміну миттєвими повідомленнями, які дозволяють користувачам створювати списки друзів та передавати статус іншому члену списку приятелів. Повідомлення про стан можуть вказувати на те, що ви розмовляєте по телефону, на важливій зустрічі, на обіді або готові поговорити.. Члени списку приятелів можуть використовувати ці повідомлення про стан “присутності”, щоб вибрати відповідний час для здійснення телефонного дзвінка, а не переривати в невідповідний час. Кілька провідних постачальників програм обміну миттєвими повідомленнями взяли на себе зобов'язання перетворити свої системи на використання програм обміну миттєвими повідомленнями взяли на себе зобов'язання перетворити свої системи на використання SIP.

Протокол управління шлюзом медіа (MGCP) та Megaco

У MGCP та Megaco функцію обробки викликів можна відокремити від функції шлюзу VoIP. Ми можемо визначити нову сутність, “агента виклику” (CA) для управління шлюзами та виконання обробки дзвінків. Фізичний продукт, що реалізує функцію агента виклику, не обов'язково повинен розташовуватися поблизу шлюзу і може керувати багатьма шлюзами. Ця стуктура спрощує продукт VoIP-шлюзу, дозволяючи шлюзу розташовуватися в будинках та невеликих офісах за низькою вартістю.

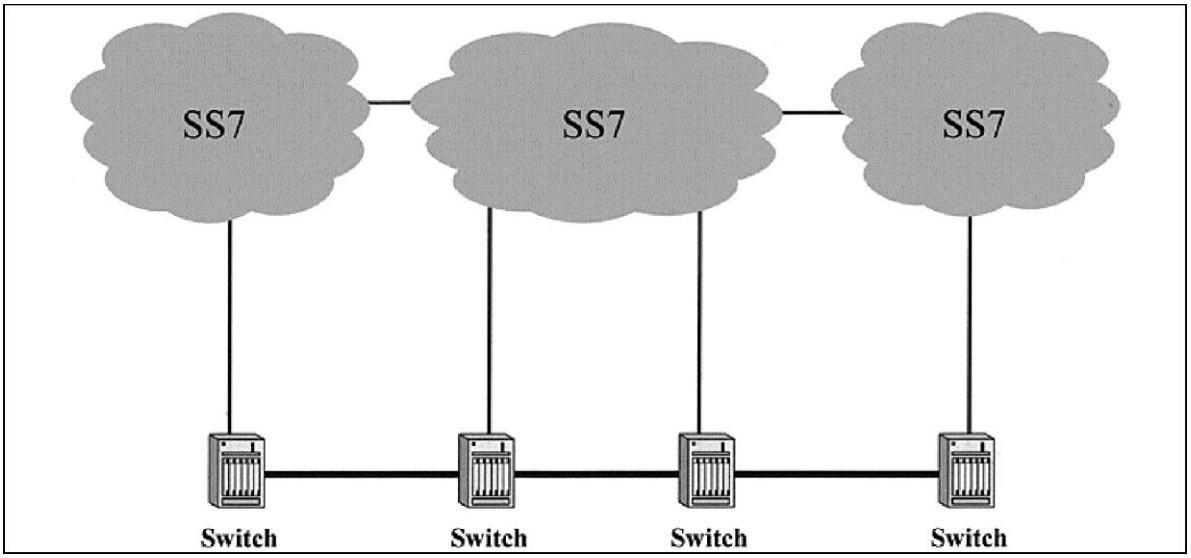

Рисунок 11 Існуючі мережі з комутацією каналів

Розглянемо схему мережі з комутацією каналів на малюнку 11. Комутатори передають телефонний трафік безпосередньо від одного до іншого, але передають інформацію про сигналізацію дзвінків між собою за допомогою окремої мережі пакетної сигналізації SS7. Зверніть увагу, що, незважаючи на пакетну комутацію, протокол SS7 не пов'язаний з IP.

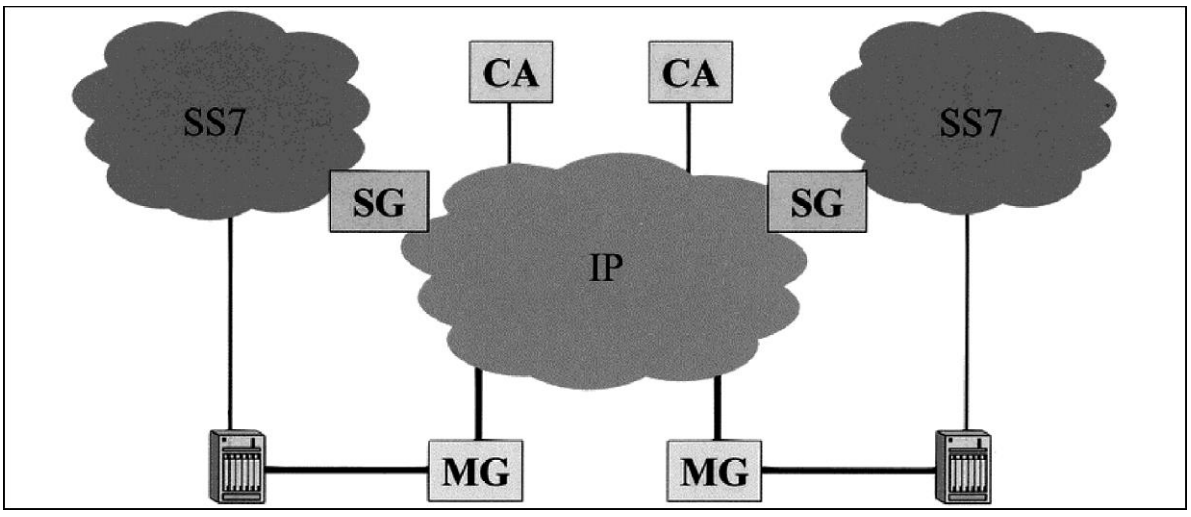

Рисунок 12 Структура ведучого / веденого за участю агентів викликів, шлюзів сигналізації та медіа.

Постачальники PSTN кажуть, що IP-телефонія повинна замінити PSTN таким чином, щоб основні функції PSTN продовжували працювати протягом тривалого періоду міграції. Це призводить до двох типів шлюзів. Медіашлюзи (MG)

приймають голосовий або «медіа» трафік від комутаторів каналів і пакетізують голос, який передається через IP-мережу. Шлюзи сигналізації (SG) з'єднують мережі сигналізації (наприклад, SS7) та мережі IP, щоб агенти викликів, підключені до мережі IP, могли зв'язуватися з комутаторами каналів, підключеними до мереж сигналізації, як показано на малюнку 12.

MG дозволяє з'єднувати різні мережі, забезпечуючи функції перетворення носіїв та / або функції перекодування. Наприклад, MG може приймати пакети з IP-мережі, депакетизувати їх, перекодувати і передавати медіапотік комутованій мережі. У деяких випадках MG може діяти як перемикач при об'єднанні двох завершень або ресурсів одного типу. Отже, інші функції, які MG може виконувати, включають міст конференції з усіма пакетними інтерфейсами, інтерактивний блок голосової відповіді або систему розпізнавання голосу. MG також підтримує функції ресурсів, включаючи сповіщення про події, розподіл та управління ресурсами, а також системні функції, такі як встановлення та підтримка зв'язку з Агентом викликів.

Функція SG знаходиться на краю мережі передачі даних, передаючи, перекладаючи або припиняючи сигнали управління дзвінками між мережею пакетних даних та мережею телефонної комутації з комутацією каналів. Шлюз SS7-IP використовував би функцію SG. З іншого боку, MG може також використовувати функцію SG для обробки традиційної телефонної сигналізації, пов'язаної із закінченням магістралі або лінії на MG, такою як канал D лінії ISDN BRI або магістраль PRI.

Агент виклику, який часто називають «контролером медіа-шлюзу» (MGC), повинен взаємодіяти з медіа-шлюзом для контролю своїх дій. Для цього типу зв'язку було розроблено кілька протоколів, включаючи простий протокол управління шлюзом (SGCP) [12], протокол управління IP-пристроями (IPDC), протокол управління медіа-шлюзом (MGCP) ([12], [4]) та Megaco /H.248 [13]. SGCP - оригінальний протокол передачі сигналів Master-slave на основі рядків ASCII для VoIP. MGCP послідував наступного року, поєднуючи характеристики SGCP та IPDC з більшими можливостями. Megaco - це подібний протокол, який IETF розробив із

ще більшими можливостями.

Хоча MGCP RFC не був документом який відслідковує стандарти, але багато постачальників реалізували шлюзи і агенти викликів з використанням MGCP. Це також основа для протоколу мережевої сигналізації викликів (NCS), розробленого групою PacketCable компанії Cable Labs [14]]. Існує кілька доступних реалізацій NCS 1.0.

І SCGP, і MGCP розроблені як розподілені системні протоколи, які надають користувачеві вигляд єдиної VoIP-системи. Вони являють собою протоколи без збереження стану в тому сенсі, що послідовність транзакцій між MG та агентом виклику може виконуватися без будь-якої пам'яті попередніх транзакцій. З іншого боку, MGCP вимагає від MGC збереження стану виклику.

І MGCP, і Megaco підтримують такі функції медіа-шлюзу:

• Створювати, модифікувати та видаляти з'єднання, використовуючи будь-яку комбінацію транзитної мережі, включаючи ретрансляцію кадру, ATM, TDM, Ethernet або аналогову. Можна встановити з'єднання для передачі аудіопакетів через кілька типів мереж-носіїв:

о IP-мережі, що використовують RTP та / або UDP;

о внутрішнє з'єднання, наприклад, задню плату TDM або шину взаємозв'язку шлюзу. Це використовується для з'єднань, які закінчуються шлюзом, але негайно перенаправляються через телефонну мережу ("шпилька з'єднання").

• Виявляти або генерувати події в кінцевих точках або з'єднаннях. Наприклад, шлюз може виявляти набрані цифри або генерувати сигнал дзвінка підключення.

• Збирайте цифри відповідно до карти цифр, отриманої від агента виклику, та надсилайте повний набір набраних цифр агенту дзвінка.

• Дозволити зміни під час розмови, такі як утримання виклику, відтворення оголошень і конференц-зв'язок.

• Звітувати статистику дзвінків.

Окрім деяких відмінностей у термінології, протокол Megaco надає агенту викликів більшу гнучкість типу транспорту та контролю над медіа-шлюзом, а та-

кож деякі гачки для таких програм, як відеоконференції. І MGCP, і Megaco забезпечують процедуру для агента виклику надсилати пакет властивостей, сигналів або подій. Megaco має визначений спосіб для агента виклику та шлюзу узгодити версію, яка буде використана, але MGCP не має механізму контролю версій, тому слід покладатися на власний процес переговорів постачальника.

У сферах безпеки та якості обслуговування Megaco є більш гнучким, ніж MGCP. Хоча MGCP підтримує лише IPSEC, Megaco також підтримує заголовок автентифікації. Обидва протоколи підтримують автентифікацію вихідної адреси. Хоча MGCP підтримує лише UDP для передачі сигналів, Megaco підтримує UDP, TCP, ATM та SCTP.

Megaco також має кращі механізми управління потоками та розподілом ресурсів.

Будь-який MGCP або Megaco (або навіть SGCP або IPDC) можуть бути використані для структури VoIP ведучого-підлеглого, особливо коли метою є управління багатьма недорогими шлюзами IP-телефонії. Для зв'язку між агентами викликів або для управління групами зовнішніх ліній може бути більш доречним SIP. У той час як MGCP і Megaco мають певні команди для управління викликами VoIP, SIP дозволяє використовувати один примітив для надання різних послуг.

Отже, SIP пропонує обіцянку підтримувати широкий спектр послуг, окрім базової телефонії, включаючи обмін миттєвими повідомленнями, управління присутністю та веб-електронну комерцію з підтримкою голосу, а SIP сприяє розробці нових програм незалежними третіми сторонами. Деякі постачальники програмних комутаторів використовують MGCP або Megaco для управління шлюзами, але використовують SIP на рівні програми [15].

Транспорт

Типові інтернет-програми використовують для зв'язку протокол TCP / IP. Хоча IP - це безпровідний протокол мережевих комунікацій, TCP - надійний транспортний протокол, який використовує підтвердження та повторну передачу для забезпечення отримання пакетів. Використовуючи разом, TCP / IP є надійним набором протоколів мережевих комунікацій, орієнтованим на підключення. TCP / IP

не підходить для спілкування в режимі реального часу, наприклад, передачі мови, оскільки функція підтвердження / повторної передачі призведе до надмірних затримок.

Тому VoIP використовує комбінацію RTP та UDP через IP. UDP забезпечує ненадійну послугу доставки без з'єднання, використовуючи IP для транспортування повідомлень між кінцевими точками в Інтернеті. RTP, що використовується спільно з UDP, забезпечує наскрізні транспортні функції мережі для додатків, що передають дані в реальному часі, такі як аудіо та відео, через одноадресну та багатоадресну мережеві послуги. RTP не резервує ресурси та не гарантує якість послуг. Супутній протокол RTCP дійсно дозволяє відстежувати лінію зв'язку, але більшість програм VoIP пропонують безперервний потік пакета RTP / UDP / IP без урахування втрати або затримки пакету в приймачі.

Затримка

Час передачі включає затримку внаслідок обробки кодеків, а також затримку розповсюдження. Рекомендація MCE-T G.114 [16] рекомендує такі односторонні обмеження часу передачі для з'єднань з адекватно контрольованим відлунням (відповідно до G.131 [17]):

• від 0 до 150 мс: прийнятно для більшості користувацьких програм;

• від 150 до 400 мс: прийнятно для міжнародних сполучень;

•> 400 мс: неприйнятно для загальних цілей планування мережі; однак визнається, що в деяких виняткових випадках ця межа буде перевищена.

Важливим є також варіація затримки, яку іноді називають тремтінням. Приймаючий шлюз або телефон повинні компенсувати зміни затримки за допомогою буфера джиттера, який накладає затримку на ранні пакети і передає пізні пакети з меншою затримкою, щоб декодований голос витікав з приймача зі стабільною швидкістю. Будь-які пакети, які надходять пізніше, ніж довжина буфера джиттера, відкидаються. Оскільки ми хочемо низьких втрат пакетів, затримка буфера джиттера - це максимальна зміна затримки, яку ми очікуємо. Ця затримка буфера джиттера повинна бути включена в загальну наскрізну затримку, яку слухач відчуває під час розмови за допомогою пакетної телефонії.

Пакетований голос має більші наскрізні затримки, ніж система TDM, що робить вищезазначені цілі затримки складними. Зразок бюджету затримки в мережі для кодека G.729 (8 кб / с) наведено в таблиці 2.

Таблиця 2. Бюджет затримки

Джерело затримки	**Внутрішній бюджет (мс)**
Захоплення зразка пристрою	0.1
Затримка кодування (Алгоритмічна затримка + затримка обробки)	17.5
Затримка пакетизації / депакатизації	20
Перейти до вихідної черги / затримки черги	0.5
Доступ (вгору) Затримка передачі посилання	10
Затримка передачі магістральної мережі	Dnw
Доступ (вниз) Затримка передачі посилання	10
Черга вводу до програми	0.5
Джиттер буфер	60
Затримка обробки декодера	2
Затримка відтворення пристрою	0.5
Разом	121.1 + Dnw

Цей бюджет не є точним. Виділена затримка буфера джиттера 60 мс є лише оцінкою; фактична затримка може бути більшою або меншою. Оскільки зразок бюджету не включає жодних конкретних затримок для стиснення та декомпресії заголовка, ми можемо вважати, що, якщо застосовуються ці функції, пов'язана затримка обробки включається в затримку каналу доступу.

Цей бюджет затримки дозволяє нам дотримуватися вказівок G.114, залишаючи 29 мс для односторонньої затримки магістральної мережі (Dnw) у національній мережі. Це досяжно в невеликих країнах. Затримки мережі в Азіатсько-

Тихоокеанському регіоні, а також між Північною Америкою та Азією можуть бути вище 100 мс. Відповідно до G.114, ці затримки є прийнятними для міжнародних зв'язків. Однак наскрізні затримки для дзвінків через VoIP значно більші, ніж для дзвінків на PSTN.

Якість голосу

Існують різні підходи до забезпечення якості обслуговування в IP-мережах. Однак перше питання полягає в тому, чи справді необхідне забезпечення якості. Деякі Інтернет-інженери стверджують, що якщо заповнюваність є низькою, то продуктивність повинна бути хорошою. По суті, дискусія ведеться про те, чи надмірна пропускна здатність мережі (включаючи пропускну здатність каналів та маршрутизатори) є менш дорогою, ніж впровадження QoS.

QoS можна досягти, керуючи чергами маршрутизаторів і маршрутизуючи трафік навколо перевантажених частин мережі. Дві ключові концепції QoS - IntServ [18] та DiffServ. Концепція IntServ полягає у резервуванні ресурсів для кожного потоку через мережу. RSVP [19] спочатку був розроблений як протокол бронювання. Коли програма вимагає певного QoS для свого потоку даних, RSVP може бути використаний для доставки запиту до кожного маршрутизатора по шляху та для підтримки стану маршрутизатора для надання запитуваної послуги. RSVP передає два типи специфікацій потоку, що відповідають правилам IntServ. Специфікація трафіку (Tspec) описує потік, а специфікація запиту на послугу (Rspec) описує послугу, що запитується, за умови, що потік відповідає Tspec. Поточні реалізації IntServ дозволяють вибрати гарантоване обслуговування або сервіс з контрольованим навантаженням.

Існує кілька причин, через які IntServ не використовується з RSVP для IP-телефонії. Незважаючи на те, що IntServ з RSVP працював би в приватній мережі для невеликих обсягів трафіку, велика кількість голосових дзвінків, які постачальники послуг IP-телефонії здійснюють у своїх мережах, підкреслила б систему IntServ RSVP. По-перше, пропускна здатність, необхідна для самого голосу, невелика, і RSVP-контроль трафіку буде становити значну частину загального трафіку. По-друге, код маршрутизатора RSVP не був розроблений для підтримки бага-

тьох тисяч одночасних з'єднань на маршрутизаторі [20].

Оскільки IntServ з RSVP погано масштабується для підтримки багатьох тисяч одночасних з'єднань, IETF розробив простішу структуру для підтримки DiffServ [18]. Структура досягає масштабованості шляхом агрегування трафіку за класифікаціями, які передаються за допомогою позначення пакетів рівня IP за допомогою поля DS у заголовках IPv4 або IPv6. Складні операції класифікації, маркування, контролю та формування повинні здійснюватися лише на межі мережі. Основною метою диференційованих послуг є надання можливості забезпечувати різні рівні обслуговування для потоків трафіку на загальній мережевій інфраструктурі. Для досягнення цього можуть бути використані різні методи управління ресурсами, але кінцевим результатом буде те, що деякі пакети отримуватимуть іншу (наприклад, кращу) послугу, ніж інші. Наприклад, це дозволить постачальникам послуг пропонувати послугу в режимі реального часу, надаючи пріоритет використанню смуги пропускання та черг маршрутизатора, аж до конфігурованого обсягу пропускної спроможності, виділеного для трафіку в реальному часі. Привабливість DiffServ полягає в тому, що він відносно простий (у порівнянні з IntServ), але надає таким програмам, як VoIP, певне покращення продуктивності в порівнянні з „IP-мережами з найкращими зусиллями”.

Ще один підхід до досягнення якості голосу - використання MPLS. MPLS пропонує IP-мереж можливість забезпечувати управління трафіком, а також диференційований сервісний підхід до якості голосу. За кілька десятиліть організація трафіку і автоматична перенаправлення телефонного трафіку підвищили ефективність і надійність PSTN. Frame Relay і ATM також пропонують можливості маршрутизації від джерела (або «явну»), які дозволяють управляти трафіком. Можна спроектувати IP-мережу для роботи поверх мережі Frame Relay або ATM («Рівень 2»), забезпечуючи деякі функції управління трафіком, але такий підхід збільшує вартість і складність експлуатації. MPLS пропонує IP-мереж можливість забезпечувати управління трафіком, а також диференційований сервісний підхід до якості голосу.

Розробник мережі VoIP може вибрати DiffServ, MPLS-TE плюс DiffServ або

DS-TE в залежності від економічної ситуації. Якщо VoIP повинен становити невелику частину загального трафіку, може бути достатньо DiffServ або MPLS-TE плюс DiffServ. DS-TE обіцяє більш ефективне використання IP-мережі, що несе велику частку VoIP-трафіку, можливо, з більшою складністю операцій [20].

Регулювання

VoIP з'являється на арені зв'язку в той час, коли регулювання телекомунікацій існує вже майже сто років. Тому важливо розуміти відповідні правила в тому вигляді, в якому вони існують, перш ніж обговорювати проблеми, які може поставити VoIP. Цей розділ забезпечує необхідний нормативний контекст та обговорює відповідні правила VoIP, як визначено у Повідомленні Федеральної комісії зв'язку (FCC) щодо послуг із підтримкою IP щодо пропонованих правил. Фактичний текст закону поміщений в рамку, і при бажанні його можна пропустити.

Законодавчі визначення та юрисдикція

Кілька визначень, викладених в Законі про зв'язок та попередніх розпорядженнях Комісії, мають значення для розуміння контексту VoIP.

По-перше, Закон визначає терміни "звичайний перевізник" та "перевізник", щоб включати " будь-яка особа, яка працює як найманий перевізник міжміським або іноземним зв'язком по дроту чи радіо ". Закон спеціально виключає з цього визначення осіб, які «займаються радіомовленням» .

Федеральна комісія зв'язку вже давно розмежовує «основні» та «розширені» пропозиції послуг. У рядку рішень про комп'ютерні запити,

комісія зазначила, що " базова " послуга - це послуга, що пропонує потужність передачі для доставки інформації без чистої зміни форми або змісту. Постачальники "базових" послуг підпадали під загальне регулювання перевізників відповідно до Розділу II Закону. На відміну від цього, «розширена» послуга містить базовий компонент послуги, але також «використовує програми для обробки комп'ютера, які діють на формат, вміст, код, протокол або подібні аспекти переданої інформації абонента; надавати абоненту додаткову, іншу або реструктуризовану інформацію; або передбачати взаємодію абонентів із збереженою інфор-

мацією ".

Комісія дійшла висновку, що посилені послуги підпорядковуються Комісії. Однак він також встановив, що розширений ринок послуг був високо конкурентоспроможним з низькими бар'єрами для входу; тому Комісія відмовилася розглядати постачальників розширених послуг як "звичайних перевізників", що підпадають під регулювання згідно з Розділом II Закону.

Закон 1996 р. Визначав "телекомунікації" як "передачу, між або серед визначених користувачем пунктів, інформації, яку обрав користувач, без зміни форми або змісту інформації, що надсилається та отримується".

Закон 1996 р. Також визначав "телекомунікаційну послугу", що означає "пропонування телекомунікацій за певну плату безпосередньо населенню або таким класам користувачів, які можуть бути ефективно доступними для громадськості, незалежно від використовуваних засобів". Комісія дійшла висновку, і суди погодились, що визначення поняття "телекомунікаційна послуга" мало на меті "пояснити, що телекомунікаційні послуги є загальними послугами перевізника".

Різні повноваження та зобов'язання, викладені в Законі, включаючи, наприклад, право на доступ до відокремлених елементів мережі діючого оператора для місцевих послуг та зобов'язання зробити мережу доступною для людей з обмеженими можливостями - поширюються лише на організації, що надають "телекомунікаційну послугу".

На відміну від цього, Закон 1996 р. Визначав "інформаційну послугу" як "пропозицію можливості генерувати, отримувати, зберігати, перетворювати, обробляти, отримувати, використовувати або робити доступною інформацію за допомогою телекомунікацій, і включає електронну публікацію, але не включає будь-яке використання будь-якої такої можливості для управління, контролю або експлуатації телекомунікаційної мережі або управління телекомунікаційною послугою ".

Закон не встановлював якихось особливих прав чи вимог щодо постачальників інформаційних послуг, але Комісія реалізувала свої допоміжні повноваження відповідно до Розділу I Закону щодо застосування вимог до інформаційних по-

слуг.

У звіті Конгресу 1998 року, відомому як "Звіт Стівенса", Комісія розглядала належну класифікацію послуг IP-телефонії відповідно до Закону 1996 року. У цьому

Як повідомляється, Комісія відмовилася робити будь-які висновки щодо належної правової та нормативної бази для розгляду цих послуг, зазначивши, що "остаточні заяви" будуть недоречними "за відсутності більш повного опису, орієнтованого на окремі пропозиції послуг".

Однак Комісія зауважила, що у випадку IP-телефонії "від комп'ютера до комп'ютера", коли "фізичні особи використовують програмне та апаратне забезпечення в своїх приміщеннях для здійснення дзвінків між двома комп'ютерами, підключеними до Інтернету", постачальник послуг не «надає» телекомунікації, і, отже, послуга не є «телекомунікаційною послугою» згідно із визначенням Закону цього поняття. На відміну від цього, послуга IP-телефонії "телефон до телефону", яка покладається на "комутовану або виділену схему ... для здійснення або припинення дзвінків в Інтернеті", здається, "несе характеристики" телекомунікаційних послуг, оскільки конкретна послуга відповідала чотирьом критеріям: (1) він заявляє, що надає послугу голосової телефонії або факсимільної передачі; (2) він не вимагає від замовника використання CPE, відмінного від CPE, необхідного для здійснення звичайного дзвінка (або факсимільної передачі) через телефонну комутаційну мережу загального користування; (3) це дозволяє клієнтові телефонувати за номерами телефонів, призначеними відповідно до Північноамериканського плану нумерації та відповідних міжнародних угод; і (4) він передає інформацію про клієнта без чистої зміни форми або змісту.

911 / E911

Згідно з правилами Комісії, існує два набори вимог до 911. Перший набір, "базовий 911", вимагає, щоб охоплені перевізники доставляли всі 911 дзвінків до відповідного пункту відповіді громадської безпеки (PSAP) або визначеного загальнодержавного пункту відповіді. Послуга Basic 911 не стосується того, яку інфо-

рмацію повинен отримувати PSAP від цього дзвінка; швидше він прагне забезпечити доставку 911 дзвінків.

Отже, Комісія також прийняла вимоги до покритих операторів бездротового зв'язку, щоб вони могли надавати номер зворотного дзвінка абонента, що телефонує, та інформацію про місцезнаходження того, хто телефонує . Ці правила, які називаються "розширеними правилами 911" (E911) Комісії, в даний час вводяться в дію по всій країні, і розгортання можливостей E911 триває.

У наказі про сферу застосування E911 зазначено, що Комісія має законодавчі повноваження відповідно до розділів 1, 4 (i) та 251 (e) (3) Закону щодо визначення суб'єктів господарювання, що підпадають під дію правил Комісії 911 та E911. Однак FCC у службі з підтримкою IP NPRM27 заявив, що "вирішуючи, чи застосовувати наші регулятивні повноваження в контексті послуг з підтримкою IP, ми пам'ятаємо, що розробка та розгортання цих служб знаходиться на ранніх стадіях, що ці послуги швидко змінюються і, ймовірно, розвиватимуться так, як ми не можемо передбачити, і накладати регулятивні мандати, особливо ті, що накладають технічні мандати, слід з обережністю ».

У зв'язку з великою різноманітністю типів трафіку в сучасних пакетних мережах і методів їх аналізу необхідно провести систематизацію наявних теоретичних досліджень з метою виявлення найбільш загальних підходів до математичного опису трафіку IP-телефонії, а також позначити області для подальших досліджень. Існує два основні підходи до дослідження трафіку IP-телефонії:

-на рівні викликів;

-на рівні пакетів.

При використанні першого підходу весь трафік в пакетної мережі розглядається як потік окремих викликів, що надходять на досліджувану систему. Такий підхід є класичним підходом до дослідження телефонних систем. При цьому не поділяють трафік сигналізації і призначених для користувача даних. Причиною цього є те, що в традиційних телефонних мережах сигналізація передавалася всередині мовного каналу і кожен канал сигналізації обслуговував єдиний мовний канал. З появою загальноканальної сигналізації ЗКС№7 [2], однак, цей підхід за-

лишився незмінним, незважаючи на те, що загальний канал, сигналізації обслуговує цілу групу (іноді кілька тисяч) мовних каналів. Спільне дослідження трафіку сигналізації і мультимедійних файлів значно спрощує завдання дослідника. Але такий підхід передбачає, що кожен вступник виклик створює однакове навантаження на досліджувану систему. Насправді кожна окрема послуга може надавати різну навантаження на реалізують її елементи. Деякі послуги вимагають передачі декількох десятків повідомлень (конференції), можуть використовувати велику смугу пропускання (широкосмугове відео), а також можуть надаватися без встановлення з'єднання як такого (передача повідомлень).

У разі дослідження трафіку на рівні викликів завдання дослідників зводиться до визначення того, наскільки трафік IP-комунікацій відрізняється від традиційного телефонного трафіку і наскільки ці відмінності (якщо такі є) змінюють основні параметри, що застосовуються при розрахунку і проектуванні мереж IP-комунікацій (наприклад, характер законів розподілу інтенсивності надходження викликів і розподілу тривалості обслуговування викликів в системі).

Другий підхід ґрунтується на тому факті, що на відміну від традиційної телефонії в мережах IP-телефонії передача будь-яких повідомлень здійснюється за допомогою технології комутації пакетів, що накладає свої особливості на досліджувані характеристики (зміна навантаження в часі, розмір буферів вузлів мережі, довжини черг в е т їх буферах і т.д.). Для дослідження трафіку IP-телефонії на рівні пакетів необхідно провести його декомпозицію для спрощення і конкретизації цілей і об'єктів дослідження [6].

Весь трафік IP-телефонії на рівні пакетів можна розділити на дві основні складові:

-трафік сигнальної інформації - трафік сигнальних повідомлень, переданих для встановлення, модифікації (зміни) і руйнування сеансу зв'язку в пакетної мережі;

-трафік користувальницької інформації - трафік передачі голосових повідомлень, відео повідомлень і даних користувачів.

Як зазначалося раніше, кожен з цих типів трафіку використовує свої прото-

коли передачі і має різні вимоги до якості обслуговування.

Роздільне дослідження трафіку сигналізації і призначеної для користувача інформації дозволяє більш точно підібрати математичну модель для даного типу трафіку. Трафік мультимедійних файлів для кожного окремого виклику являє собою безперервну послідовність пакетів в обох напрямках, в той час як трафік сигналізації-асинхронний діалог, що складається з невеликих повідомлень, переданих, в загальному випадку, в початку і кінці з'єднання. Таким чином, очевидно, що така декомпозиція має сенс, і результати дослідження кожного типу трафіку повинні розглядатися окремо.

Дослідження трафіку IP-телефонії на рівні викликів

Як зазначалося вище, завдання дослідження трафіку на рівні викликів зводиться до визначення двох його основних характеристик:

- ймовірнісному закону розподілу інтенсивностей викликів, що надходять на досліджувану систему;

-ймовірнісному закону розподілу тривалості цих викликів.

У ряді робіт [4] показано, що інтенсивність надходження викликів в досліджувану систему має експоненціальне розподіл, а автокореляційна функція показує, що надійшли виклики взаємно незалежні, тому робиться висновок, що інтенсивність надходження викликів досить добре може описуватися класичної пуассонівскою моделлю.

Розподіл тривалості між викликами в більшості робіт оцінюється як статечне, що підкоряється закону Парето, лог-нормальному розподілу [4] та інших. Різниця отриманих законів розподілу, швидше за все, пояснюється різними розмірами досліджуваних мереж (з 4 і більше пристроїв на декількох діючих мережах), тривалістю збору статистики і характером навантаження.

В цілому, більшість результатів дослідників сходяться до одного: розподіл інтенсивності викликів добре описується пуассонівскою моделлю, в той час як розподіл тривалості викликів краще описується статечними розподілами, а не експонентними, як це вважалося раніше. Конкретний вид статечного розподілу залежить від масштабу і структури мережі.

Дослідження трафіку на рівні пакетів

Як згадувалося вище для дослідження трафіку IP-телефонії на рівні пакетів доцільніше розглядати окремо сигнальний трафік і трафік для користувача інформації (трафік мультимедійних файлів), так як в пакетних мережах ці два види трафіку можуть передаватися за різними маршрутами, мати різні закони розподілу часових параметрів і оброблятися різними вузлами мережі.

Аналіз досліджень трафіку передачі відеоданих

Трафік мультимедійних файлів в загальному випадку може складатися з декількох типів трафіку:

-мовної (голосовий) трафік;

-відеотрафік;

-трафік обміну миттєвими повідомленнями (1М-трафік);

-трафік даних (web, факси та ін.).

Останні два типи представляють мало інтересу для дослідження, оскільки є протоколами відкладеного (не реальну) часу, обсяг переданих даних відносно невеликий (IM-трафік, факси) або вимоги до QoS досить низькі (web) - дослідження IM-трафіку проводяться в сукупності з мовним трафіком.

Значне число робіт присвячено дослідженню потоків відеотрафіка зі змінною швидкістю VBR (Variable Bit Rate) [2]. Основними результатами цих робіт є:

-визначено наявність ефекту самоподібності в відеотрафік;

-визначено, що розподіл довжин пакетів, що містять закодовану інформацію, підкоряється закону Парето;

-підтверджено, що довгострокова залежність є невід'ємною частиною відеотрафіка і присутній в ньому в незалежності від типу використовуваного видеокодека.

Однак більшість робіт присвячено дослідженню мовного трафіку реального часу. В рекомендації P.59 [7] міжнародного союзу електрозв'язку ITU-T описаний сигнал, за своїми статистичними характеристиками нагадує людську мову. Цей сигнал відображає такі основні особливості людської мови, як періоди активності одного або обох мовців (ON-періоди) і періоди, коли один або обидва учасники

розмови мовчать (OFF-періоди). Розподіл тривалості таких періодів як передбачалося раніше, є експоненціальним. Однак, як показали проведені експерименти, таке припущення дійсно не завжди. У різних випадках дослідники довели, що розподіл тривалості періодів ON/OFF підпорядковується розподілу Парето, Гамма розподілу [5], розподілу Вейбула, лог-нормальному розподілу [7] та інших. Такі відмінності можуть бути обумовлені різними розмірами досліджуваних мереж, різними обсягами трафіку, індивідуальними особливостями мовців, механізмами визначення голосової активності VAD (Voice Active Detection) і ін.

В цілому більшість робіт сходяться на кількох основних висновках про розподіли тривалості періодів ON/OFF:

-розподіл є скоріше статечним з "важким хвостом", а не експоненціальним, як це передбачалося раніше;

-закони розподілу тривалості періодів ON і OFF можуть відрізнятися;

-зазвичай періоди OFF більш, ніж періоди ON, що пояснюється особливістю людської мови;

-вибір конкретного закону розподілу повинен здійснюватися в кожному випадку індивідуально, так як він залежить від багатьох факторів;

-закон розподілу не залежить від типу використовуваного кодека [8].

Довготривала залежність в розподілах тривалості ON/OFF періодів накладає свої особливості при проектуванні мереж і розрахунку характеристик пристроїв. Вимоги до розміру буферів і довжині черг для трафіку, що володіє самоподібними властивостями, набагато вище, ніж у трафіку, заснованого на пуассонівскому процесі. Це пояснюється сильною автокореляцією самоподібного трафіку, а також наявністю "важких хвостів" в розподілі тривалості розмовних періодів. Таким чином, можна сказати, що трафік мультимедійних файлів має сильні самоподібні властивості. Але велика різноманітність особливостей, що впливають на вибір конкретного розподілу, свідчить про занадто складну структуру трафіку і робить задачу розрахунку пропускної здатності мережі, індивідуальної в кожному конкретному випадку.

Аналіз досліджень сигнального трафіку

Сигнальний трафік досліджувався значно рідше, ніж медіатрафік, однак за важливістю він ні в чому не поступається останньому. Перевантаження на окремих вузлах обробки сигнальних повідомлень або у всій мережі в цілому можуть привести до затримки або навіть до неможливості встановити з'єднання. Якість більшості телекомунікаційних послуг і користувальницьких додатків в істотній мірі визначається якістю функціонування мережі сигналізації. Звідси можна зробити висновок, що сигнальний трафік не менш важливий при проектуванні і обслуговуванні мережі, ніж медіатрафік.

Велика частина досліджень сигнального трафіку пов'язана з сигналізацією ЗКС№7. Незважаючи на те, що дана сигналізація в «чистому» вигляді не використовується в IP-мережі, деякі її особливості роблять схожою на різні типи сигналізацій IP-комунікацій:

-всі повідомлення сигналізації ЗКС №7 передаються у вигляді пакетів і повідомлень, а сама «накладена» загальноканальна мережа може розглядатися як мережа з комутацією пакетів;

-процес обміну сигнальними повідомленнями на різних рівнях стека ЗКС№7 дуже схожий на відповідні процеси в різних системах сигналізації IP-телефонії (H.323, H.323);

-в деяких випадках потрібна передача повідомлень протоколу ЗКС№7 по мережах IP, для чого існують кілька транспортних протоколів (SIGTRAN,H.323).

Найбільш суттєві висновки щодо характеру трафік мережі ЗКС№7 на рівні повідомлень:

-автокорреляция процесу має форму повільно спадної залежності;

-дисперсія самого процесу і процесу, утвореного від вихідного шляхом усереднення за часом, убуває повільніше величини, зворотної інтервалу усереднення;

-дуже важливою є вивчення зміни швидкості надходження на досліджувану систему повідомлень на невеликих масштабах часу (3-10 секунд);

-«тяжкохвостовий» розподіл тривалості викликів зберігає свою форму в періоди великої і малої навантаження, в різних масштабах часу;

-затримки при обробці в вузлах сигналізації, повторні передачі повідомлень

по закінченні тайм-ауту, збої в маршрутизації і нестандартні процеси обміну повідомленнями дуже впливають на навантаження в мережі і її характеристики.

В цілому більшість висновків цієї роботи, говорить про те, що на рівні пакетів трафік ЗКС№7 володіє довготривалої залежністю. Аналогічне дослідження було проведено в [7], однак об'єктом дослідження був трафік ЗКС№7 не тільки фіксованих, але і мобільних мереж між двома центрами комутації мобільного зв'язку MSC (Mobile Switching Center). Результати аналізу аналогічні з використанням методу авторегресійного проінтегрування змінного середнього (АРПСС), що дозволяє робити прогноз трафіку. В результаті, відхилення прогнозованого трафіку ЗКС№7 від реального в годину пік не перевищували 7,14% у фіксованій мережі і 7,83 %-в мобільній.

Найпростіші методи розрахунку сигнального навантаження мережі ЗКС№7 враховують лише деякі параметри мережі, такі як число каналів, що обслуговуються ланкою сигналізації, середнє число/довжина сигнальних одиниць для вдалих/невдалих викликів та інші. При доповнені методиками розрахунку, що дозволяють враховувати властивість мобільності абонентів, нерівність сигнальної навантаження в прямому і зворотному напрямку, тип запитуваних інтелектуальних послуг на базі технології CAMEL (Customized Application for Mobile Enhanced Logic), а також навантаження від передачі повідомлень SMS (Short Message Service).

Як вже говорилося вище, існує кілька способів передачі сигналізації ЗКС№7 по IP мережам. Основними з них є використання стека протоколів SIGTRAN і протокол H.323. Стек протоколів SIGTRAN використовує протокол SCTP як протокол транспортного рівня. Для SCTP була розроблена математична модель його функціонування, що застосовується далі для розрахунку затримки передачі повідомлень SIGTRAN. Дана модель була доопрацьована для обліку формування пакету SCTP за таймером.

Ще одним способом передачі сигналізації ЗКС№7 по IP-мереж є протокол H.323. Повідомлення ЗКС передаються шляхом інкапсулювання в полі протоколу SDP відповідних повідомлень H.323. В для аналізу якісних показників роботи

протоколуH.323 розраховувалися розмір черги сигнальних повідомлень (розмір буфера), середня затримка в черзі і її варіація. Для цього в якості моделі черзі використовувалася система масового обслуговування (СМО) типу M/G/1 з пріоритетним обслуговуванням. В результаті порівняння теоретичних і експериментальних даних був зроблений висновок про достатню точність розроблених моделей і про можливість їх використання на етапі планування і проектування транзитних мереж операторського класу, що використовують протокол H.323.

Як уже згадувалося раніше, одним з найпопулярніших протоколів в мережах IP-телефонії є H.323. Варто зазначити, що протокол H.323 має величезне число розширень, що дозволяють не тільки встановити просте голосове або відео з'єднання між двома абонентами, а й зібрати багатоточкову конференцію, передавати миттєві повідомлення IM, контролювати доступність абонента (Presence), реєструвати кілька абонентських терміналів (фіксованих або мобільних) з одним номером і безліч інших. Оскільки набори послуг, реалізовані в різних мережах H.323, можуть відрізнятися, це може надати істотний вплив на профіль трафіку H.323 [9].

Одним з популярних методів дослідження трафіку мережі H.323 є симулювання роботи даного протоколу в різних середовищах (наприклад, NS-2, OMNeT, NetSim і ін.) За допомогою машини з кінцевим числом станів FSM (Finite State Machine). У загальному випадку модель роботи протоколу H.323 може описуватися «закритою мережею». Закрита мережа являє собою кілька вузлів, кожен з яких відповідає певному стану H.323-сессії в процесі встановлення або руйнування найпростішого голосового з'єднання, наприклад, очікування попереднього або остаточного відповіді, очікуванню підтвердження отримання повідомлення (не враховуються стану реєстрації, аутентифікації, пересилання повідомлень, розмноження повідомлень (H.323-forking) і ін.). Кожному переходу з одного стану в інший відповідає певна ймовірність, яка грунтується на даних, отриманих з моделі транспортної IP-мережі. За допомогою симуляції можуть бути проаналізовані різні характеристики мережі H.323. Наприклад, в [5] було отримано спрощений (через реалізацію не всіх можливих станів сесії H.323 та деяких припущень щодо

транспортної мережі) метод визначення середнього числа відмов викликів, одержуваного з ймовірності скидання виклику. До того ж отримана модель була розширена до моделі симуляції роботи H.323 в бездротових мережах, шляхом введення додаткової ймовірності хорошого (поганого) прийому сигналу. Також з допомогою симуляції може бути оцінена затримка встановлення з'єднання через ретрансляції повідомлень за таймером.

Іншим способом дослідження трафіку H.323 є аналіз реального трафіку, зібраного з діючої мережі. Однак робіт, які досліджували реальний сигнальний трафік протоколу H.323, досить мало, також, як і цінних результатів. Так, на прикладі двох мереж H.323 різного масштабу (від 2 до 57 користувачів) виявлено, що на рівні пакетів H.323-трафік досить точно описується експоненціальним (Deleted розподілом також встановлено, що параметри QoS сигнального трафіку (затримка встановлення з'єднання, кількість зірваних з'єднань і ін.). Відчувається незначне погіршення, якщо трафік даних, який передається в тому ж середовищі, що і телефонний, не перевищує 70-80% від загальної пропускної здатності мережі. Також можна говорити про належність трафіку H.323 до важкохвостих розподілів. Однак велика величина інтервалів аналізу (кілька сот хвилин) робить ці висновки малопридатними для застосування на діючих мережах, де час реакції мережевих пристроїв повинно бути скорочено до мінімуму.

Однією з цікавих завдань при дослідженні трафіку H.323 є забезпечення безпеки роботи мережі. У зв'язку з повсюдним розвитком Інтернету, забезпечення безпеки мережевої інфраструктури стає однією з пріоритетних задач сервіс провайдерів. Кожна людина, отримавши доступ в мережу, може просканувати мережевий простір операторів зв'язку на предмет наявності відкритих портів. Протокол H.323 використовує стандартний порт UDP 5060, тому зловмиснику буде не важко за короткий час визначити всі пристрої в мережі, що підтримують протокол H.323. До того ж, однією з особливостей сканування є те, що в повідомленні-відповіді на скануючий запит, багато пристроїв за замовчуванням включають заголовок, який вказує не тільки виробника пристрою, але і версію ПО. Зловмисник може володіти відомостями про уразливість даної версії ПЗ і спробувати їх екс-

плуатувати. Крім цього існує цілий ряд так званих man-in-the-middle атак, в яких зловмисник вклинюється в сигнальний тракт передачі повідомлень і може змінювати або пасивно записувати весь обмін сигнальної інформації. Своєчасне виявлення цих атак істотно підвищить доступність, надійність і стійкість роботи мереж H.323. Крім стандартних рішень на основі прикордонних контролерів сесій SBC (Session Border Controller) необхідні додаткові методи виявлення атак. В роботі [7] розроблено метод виявлення DoS атак на основі особливостей протоколу H.323. При вивченні уразливості в процесі аутентифікації в мережах IMS, які працюють на базі протоколу H.323, основі статистичного аналізу трафіку H.323 були розроблені методи виявлення спотворених повідомлень і спам-атак.

Іншим, дуже важливим завданням при дослідженні трафіку H.323, є захист мережі від перевантажень [6]. Саме перевантаження вузлів мережі H.323 можуть привести до затримки встановлення сеансу зв'язку через скидання пакетів і їх ретрансляції. Існують перевантаження в мережі, які викликані одночасною спробою безлічі H.323 терміналів зробити реєстрацію на сервері. За допомогою спеціально розробленої імітаційної моделі можна встановити, що збільшення паузи між ретрансляцією повторних запитів на реєстрацією, як способом боротьби з перевантаженістю сервера, менш ефективно, ніж нарощування продуктивності обладнання. Результати імітаційного моделювання показали, що застосування порогів в буфері обробки повідомлень H.323 для запобігання перевантажень дозволяє скоротити час встановлення сеансу зв'язку і ймовірність руйнування виклику майже в 10 разів.

Незважаючи на свою важливість, проблема перевантажень в мережі сигналізації H.323 виявилася однією з найбільш маловивчених. Оскільки перевантаження в мережі сигналізації впливають на основний параметр якості обслуговування-затримки встановлення з'єднань, необхідно розуміти, що є причинами перевантаження і як з ними боротися. У наступному розділі більш детально розглянуто існуючий метод боротьби з перевантаженнями і його недоліки.

3 АЛГОРИТМИ ПОБУДОВИ МЕРЕЖ IP-ТЕЛЕФОНІЇ НА ОСНОВІ ПРОТОКОЛІВ SIP-T

3.1 Алгоритми кодування мовної інформації

Показники якості IP-телефонії

Традиційні телефонні мережі комутують електричні сигнали з гарантованою смугою пропускання, достатньою для передачі сигналів голосового спектру. При фіксованій пропускній спроможності передаваного сигналу ціна одиниці часу зв'язку залежить від віддаленості і розташування точок виклику і місця відповіді.

Мережі з комутацією пакетів не забезпечують гарантованої пропускної спроможності, оскільки не забезпечують гарантованого шляху між точками зв'язку.

Для додатків, де не важливий порядок і інтервал приходу пакетів, наприклад, e-mail, час затримок між окремими пакетами не має вирішального значення. IP-телефонія являється однією з областей передачі даних, де важлива динаміка передачі сигналу, яка забезпечується сучасними методами кодування і передачі інформації, а також збільшенням пропускної спроможності каналів, що призводить до можливості успішної конкуренції IP-телефонії з традиційними телефонними мережами.

Основними складовими якості IP-телефонії являються (рис. 3.1):

- Якість мови, яка включає:
  - діалог - можливість користувача зв'язуватися і розмовляти з іншим користувачем в реальному часі і повнодуплексному режимі;
  - розбірливість - чистота і тональність мови;
  - ехо-камера - чутність власної мови;
  - рівень - гучність мови.
- Якість сигналізації, що включає:

- встановлення виклику - швидкість успішного доступу і час встановлення з'єднання;
- завершення виклику - час відбою і швидкість роз'єднання;
- DTMF - визначення і фіксація сигналів багаточастотного набору номера.

Чинники, які впливають на якість IP-телефонії, можуть бути розділені на дві категорії:

- Чинники якості IP-мережі:
  - максимальна пропускна спроможність - максимальна кількість корисних і надлишкових даних, які вона передає;
  - затримка - проміжок часу, потрібний для передачі пакету через мережу; джиттер - затримка між двома послідовними пакетами;
  - втрата пакету - пакети або дані, втрачені при передачі через мережу.
- Чинники якості шлюзу:
  - необхідна смуга пропускання - різні вокодери вимагають різну смугу. Наприклад, вокодер G.723 вимагає смуги 16,3 кбіт/с для кожного мовного каналу;
  - затримка - час, необхідний цифровому сигнальному процесору DSP або іншим пристроям обробки для кодування і декодування мовного сигналу;
  - буфер джиттера - збереження пакетів даних до тих пір, поки усі пакети не будуть отримані і можна буде передати в необхідній послідовності для мінімізації джиттера;
  - втрата пакетів - втрата пакетів при стискуванні і/або передачі в устаткуванні IP-телефонії;
  - пригнічення ехо-камера - механізм для пригнічення ехо-камера, що виникає при передачі по мережі; управління рівнем - можливість регулювати гучність мови.

Якість передачі мови	Якість передачі сигналізації

Вплив мережі на показники якості IP-телефонії

Затримка

Затримка створює незручність при веденні діалогу, приводить до перекриття розмов і виникнення ехо-камеру. Ехо-камера виникає у разі, коли відбитий мовний сигнал разом з сигналом від видаленого кінця повертається знову у вухо того, що говорить. Ехо-камера стає важкою проблемою, коли затримка в петлі передачі більша, ніж 50 мс. Оскільки ехо-камера являється проблемою якості, системи з пакетною комутацією мови повинні мати можливість управляти ехо-камера і використовувати ефективні методи ехопридушення.

Утруднення діалогу і перекриття розмов стають серйозним питанням якості, коли затримка в одному напрямі передачі перевищує 250 мс. Можна виділити наступні джерела затримки пакетної передачі мови з кінця в кінець (рис. 3.2).

- Затримка накопичення (іноді називається алгоритмічною затримкою) ця затримка обумовлена необхідністю збору кадру мовних відліків, виконувана в мовному кодері. Величина затримки визначається типом мовного кодера і змінюється від невеликих величин (0,125 мкс) до декількох мілісекунд. Наприклад, стандартні мовні кодери мають наступну тривалість кадрів:

G.729 CS - ACELP (8 кбіт/с) - 10 мс

G.723.1 - Multi Rate Coder (5,3; 6,3 кбіт/с) - 30 мс.

- Затримка обробки - процес кодування і збору закодованих відліків в пакети для передачі через пакетну мережу створює певні затримки. Затримка кодування або обробки залежить від часу роботи процесора і використовуваного типу алгоритму обробки. Для зменшення завантаження пакетної мережі звичайні декілька кадрів мовного кодера об'єднуються в один пакет. Наприклад, три кадри кодових слів G.729, відповідних 30 мс мови, можуть бути об'єднані для зменшення розміру одного пакету.

- Мережева затримка - затримка обумовлена фізичним середовищем і протоколами, використовуваними для передачі мовних даних, а також буферами, використовуваними для видалення джиттера пакетів на приймальному кінці. Мережева затримка залежить від місткості мережі і процесів передачі пакетів в мережі.

Час затримки при передачі мовного сигналу можна віднести до одного з трьох рівнів :

- перший рівень до 200 мс - відмінна якість зв'язку. Для порівняння, в телефонній мережі загального користування допустимі затримки до 150-200 мс;
- другий рівень до 400 мс - вважається хорошою якістю зв'язку. Але якщо порівнювати з якістю зв'язки по мережах ТМЗК, то різниця буде видна. Якщо затримки постійно утримується на верхній межі 2-го рівня (на 400 мс), то не рекомендується використовувати цей зв'язок для ділових переговорів;
- третій рівень до 700 мс - вважається прийнятною якістю зв'язку для ведення неділових переговорів. Така якість зв'язку можлива також при передачі пакетів по супутниковому зв'язку.

Якість Інтернет-телефонії потрапляє під 2-3 рівні, причому неможливо упевнено сказати, що той або інший провайдер Інтернет-телефонії працює по другому рівню, оскільки затримки в мережі Інтернет мінливі. Точніше можна сказати про провайдерів IP-телефонії, що працюють по виділених каналах. Вони потрапляють під 1-2 рівні. Також необхідно враховувати затримки при кодуванні/декодуванні голосового сигналу. Середні сумарні затримки при використанні IP-телефонії зазвичай знаходяться в межах 150-250 мс.

У мережі Інтернет затримки пакетів істотно залежать від часу. Крива цієї залежності має великий динамічний діапазон і швидкість зміни. Помітні зміни часу поширення можуть статися упродовж одного нетривалого сеансу зв'язку, а коливання часу передачі можуть бути в діапазоні від десятків до сотень мілісекунд і навіть перевищувати секунду.

Важливо відмітити той факт, що затримки в мережах з комутацією пакетів впливають не лише на якість передачі мовного трафіку в реальному часі. Не менш важливо і те, що ці затримки в певних ситуаціях можуть порушити правильність функціонування телефонної сигналізації в цифрових трактах E1/T1 на стику голосових шлюзів з устаткуванням комутованих телефонних мереж. Причиною цього можна назвати той факт, що набір рекомендацій H.323 у момент своєї появи в

1997 р. був орієнтований на мультимедійні застосування, що здійснюють аудіо і відеоконференцзв'язок через мережі IP. Це рішення дозволяло значно понизити вартість таких систем в порівнянні з їх аналогами, що працюють в мережах традиційної телефонії з комутацією каналів. В процесі виділення IP-телефонії в самостійний напрям і розвитку її до послуги операторського рівня виникла необхідність з'єднання IP-шлюзів з телефонними станціями ТМЗК по цифрових трактах E1/T1. При цьому, шлюзи здійснюють взаємодію з цифровими АТС, використовуючи стандартні механізми телефонної сигналізації Q.931, інтерпретовані через команди H.225 і трансльовані в IP-мережі з використанням протоколу TCP. Згідно рекомендації Q.931, при встановленні телефонного з'єднання значення часових затримок між фазами виконання команд сигналізації строго регламентовані. Проте, при інтерпретації в IP-шлюзах команд телефонної сигналізації Q.931 стеком H.225/TCP, затримки, що виникли на шляху проходження сигналу, збільшують задані часові інтервали між командами Q.931, і в більшості випадків порушують цілісність функціонування цього протоколу. Хоча версія 2 набори рекомендацій H.323 у фазі 2 передбачає процедуру H.323 v2 Fast Connect, прискорюючу обробку команд Q.931 стеком H.225/TCP, затримки IP -каналу, особливо характерні для інфраструктури Інтернет, можуть свідомо перевищувати усі допустимі значення часових інтервалів протоколу Q.931. Цю обставину можна розцінювати як ще один аргумент на користь використання виділених каналів при побудові мереж IP-телефонії.

Джиттер

Коли мова або дані розбиваються на пакети для передачі через IP-мережу, пакети часто прибувають в пункт призначення в різний час і в різній послідовності. Це створює розкид часу доставки пакетів (джиттер). Джиттер призводить до специфічних порушень передачі мови, чутних як тріски і клацання. Розрізняють три форми джиттера :

1. джиттер, залежний від даних (Data Dependent Jitter - DDJ), - відбувається у разі обмеженої смуги пропускання або при порушеннях в мережевих компонентах;

2. спотворення робочого циклу (Duty Cycle Distortion - DCD) - обумовлено затримкою поширення між передачею від низу до верху і зверху вниз;

3. випадковий джиттер (Random Jitter - RJ) - являється результатом теплового шуму.

На рис. 3.3 приведені гістограми джиттера пакетів в локальній мережі і в мережі Інтернет з різними швидкостями роботи, що показують емпіричні розподіли вірогідності затримок. На осі абсцис відкладена відносна затримка, що характеризує реальне положення пакету в послідовності на тимчасовій осі по відношенню до ідеального в припущенні, що перший пакет прийшов без затримки.

Величини виникаючих затримок і їх вірогідності важливі для організації процедури обробки і вибору параметрів обробки. Зрозуміло, що часова структура мовного пакетного потоку міняється. Виникає необхідність організації буфера для перетворення пакетної мови, обтяженої нестаціонарними затримками в каналі, можливими перестановками пакетів, в безперервний природний мовний сигнал реального часу. Параметри буфера визначаються компромісом між величиною запізнювання телефонного сигналу в режимі дуплексного зв'язку і відсотком втрачених пакетів. Втрата пакетів являється іншим серйозним негативним явищем в IP-телефонії.

Втрата пакетів

Втрачені пакети в IP-телефонії порушують мова і створюють спотворення тембру. У існуючих IP-мережах усі голосові кадри обробляються як дані. При пікових навантаженнях і перевантаженнях голосові кадри відкидатимуться, як і кадри даних. Проте кадри даних не пов'язані з часом і відкинуті пакети можуть бути успішно передані шляхом повторення. Втрата голосових пакетів, у свою чергу, не може бути заповнена у такий спосіб і в результаті станеться неповна передача інформації. Передбачається, що втрата до 5% пакетів непомітна, а понад 10-15% - недопустима. Причому ці величини істотно залежать від алгоритмів компресії/декомпресії.

На рис. 3.4 представлені гістограми втрат пакетів. По осі абсцис відкладено

число підряд втрачених пакетів. Аналіз гістограми показує, що найбільш вірогідні втрати одного, двох і трьох пакетів. Втрати великих пачок пакетів рідкісні.

Істотно, що втрата великої групи пакетів приводить до безповоротних локальних спотворень мови, тоді як втрати одного, двох, трьох пакетів можна намагатися компенсувати.

Інтуїтивно ясно, що з підвищенням трафіку зростають затримки і втрати в телефонному каналі. В умовах обмежених пропускних здібностей це проявляється не лише при інтегральному збільшенні завантаження каналів, наприклад, в години найбільшого навантаження, але і при збільшенні потоку локального джерела інформації. Криві графіків рис. 3.3 і 3.4, побудовані для різних швидкостей передачі інформації, переконливо свідчать про необхідність використання як можна нижчих швидкостей передачі мовної інформації при природній вимозі забезпечення бажаної якості телефонного зв'язку.

Взаємозв'язок методів забезпечення якості IP-телефонії, показників якості мережі і якості виклику представлена на рис. 3.3.

Процедури обробки мови в IP-телефонії

Для забезпечення якісної передачі мовних сигналів в IP-телефонії потрібна їх наступна обробка.

1. Усунення усіх небажаних компонентів з вхідного аудіосигналу. Після оцифрування мови необхідно видалити ехо-камеру з динаміка в мікрофон, кімнатну ехо-камеру і безперервний фоновий шум (наприклад, шум від вентиляторів), а також відфільтрувати шуми змінного струму на низьких частотах звукового спектру.

Ефективне ехопридушення і зменшення шумів абсолютно потрібне в будь-якій конфігурації з "відкритим мікрофоном" і з гучномовцем на базі ПК для традиційної і IP-телефонії. Ці функції усі більшою мірою реалізуються аудіокомпонентами ПК, так що сама система IP-телефонії може їх і не мати. Шлюзам IP-телефонії вимагається виконувати менший об'єм попередньої обробки, ніж кінце-

вим рішенням, тому що АТС і телефонна мережа забезпечують фільтрацію і зменшення шумів.

2. Пригнічення пауз в мові; розпізнавання залишкового фонового шуму (зовнішніх шумів) і кодування для відновлення на далекому кінці; те ж саме для пізнаваних сигналів. Паузи краще всього повністю пригнічувати на ближньому кінці. Для збереження навколишніх звуків необхідно змоделювати фонові шуми, щоб система на далекому кінці могла відновити їх для слухача. Сигнали багаточастотного набору номера DTMF і інші сигнали можна замінити на короткі коди для відновлення на далекому кінці (чи для безпосередньої обробки). Можливі проблеми: через те, що функція пригнічення пауз активізується, коли гучність мови стає нижче певного порогу, деякі системи обрізують начала і кінці слів (у періоди наростання і зниження енергії мови).

3. Стискування голосових даних. Стискувати оцифрований голос можна різними способами. У ідеалі рішення, використовувані для IP-телефонії, мають бути досить швидкими для виконання на недорогих цифрових сигнальних процесорах DSP, зберігати якість мови і давати на виході невеликі масиви даних.

4. "Нарізування" стислих голосових даних на короткі сегменти рівної довжини, їх нумерація по порядку, додавання заголовків пакетів і передача. Хоча стек протоколів TCP/IP підтримує пакети змінної довжини, їх використання утрудняє досягнення стійкої і передбачуваної міжмережевої маршрутизації в голосових застосуваннях. Маршрутизатори швидко обробляють невеликі пакети і розглядають зазвичай усі передавані по одній і тій же IP-адресі пакети одного розміру однаковим чином. В результаті пакети проходять по одному маршруту, тому їх не потрібно переупорядковувати.

5. Прийом і переупорядковування пакетів в адаптивному "буфері ресинхронізації" для забезпечення інтелектуальної обробки втрат або затримок пакетів. Головною метою тут являється подолання впливу змінної затримки між пакетами. Вирішення цієї проблеми полягає в буферизації достатнього числа пакетів (при відкладеному їх відтворенні), що надходять, з тим, щоб відтворення було безперервним, навіть якщо час між вступом пакетів сильно різниться. Кращі продукти

для IP-телефонії моделюють продуктивність мережі і регулюють розмір буфера ресинхронізації відповідним чином - зменшуючи його (скорочуючи затримку перед відтворенням), коли мережа поводиться передбачуваним чином, і збільшуючи в протилежній ситуації.

Алгоритми кодування мовної інформації

Одним з важливих чинників ефективного використання пропускної спроможності IP-канала, являється вибір оптимального алгоритму кодування/декодування мовної інформації - кодека.

Усі існуючі сьогодні типи мовних кодеків за принципом дії можна розділити на три групи:

1. Кодеки з імпульсно-кодовою модуляцією (ІКМ) і адаптивною диференціальною імпульсно-кодовою модуляцією (АДІКМ), що з'явилися у кінці 50-х років і використовуються сьогодні в системах традиційної телефонії. В більшості випадків, є поєднанням АЦП/ЦАП.

2. Кодеки з вокодерним перетворенням мовного сигналу виникли в системах мобільного зв'язку для зниження вимог до пропускної спроможності радіотракту. Ця група кодеків використовує гармонійний синтез сигналу на підставі інформації про його вокальні складові - фонеми. В більшості випадків, такі кодеки реалізовані як аналогові пристрої.

3. Комбіновані (гібридні) кодеки поєднують в собі технологію вокодерного перетворення/синтезу мови, але оперують вже з цифровим сигналом за допомогою спеціалізованих DSP. Кодеки цього типу містять в собі ІКМ або АДІКМ кодек і реалізований цифровим способом вокодер.

На рис. 3.6 представлена усереднена суб'єктивна оцінка якості кодування мови для вищеперелічених типів кодеків.

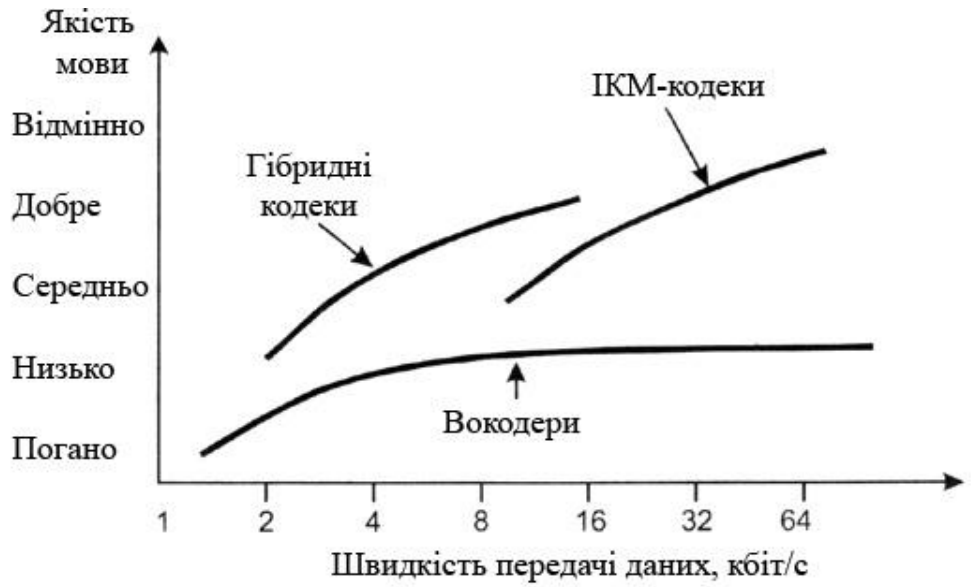

Рисунок 3.6 - Усереднена суб'єктивна оцінка якості кодування мови для різних типів кодеків

У голосових шлюзах IP-телефонії поняття кодека має на увазі не лише алгоритми кодування/декодування, але і їх апаратну реалізацію. Більшість кодеків, використовуваних в IP-телефонії, описані рекомендаціями сімейства "G" стандарту H.323 (рис. 3.7).

Усі методи кодування, засновані на певних припущеннях про форму сигналу, не підходять при передачі сигналу з різкими скачками амплітуди. Саме такий вид має сигнал, генерований модемами або факсимільними апаратами, тому апаратура, що підтримує стискування, повинна автоматично розпізнавати сигнали факс-апаратів і модемів і обробляти їх інакше, ніж голосовий трафік. Багато методів кодування беруть свій початок від методу кодування з лінійним пророкуванням LPC (Linear Predicative Coding). Як вхідний сигнал в LPC використовується послідовність цифрових значень амплітуди, але алгоритм кодування застосовується не до окремих цифрових значень, а до певних їх блоків. Для кожного такого блоку значень обчислюються його характерні параметри: частота, амплітуда і ряд інших. Саме ці значення і передаються по мережі. При такому підході до кодування мови, по-перше, зростають вимоги до обчислювальних потужностей спеціалізованих процесорів, використовуваних для обробки сигналу, а по-друге, збіль-

шується затримка при передачі, оскільки кодування застосовується не до окремих значень, а до деякого їх набору, який перед початком перетворення слід накопити в певному буфері.

Важливо, що затримка в передачі мови пов'язана не лише з необхідністю обробки цифрового сигналу (цю затримку можна зменшувати, збільшуючи потужність процесора), але і безпосередньо з характером методу стискування. Метод кодування з лінійним пророкуванням LPC дозволяє досягати дуже великих ступенів стискування, яким відповідає смуга пропускання 2,4 або 4,8 кбіт/с, проте якість звуку тут сильно страждає. Тому в комерційних додатках він не використовується, а застосовується в основному для ведення службових переговорів. Складніші методи стискування мови засновані на застосуванні LPC у поєднанні з елементами кодування форми сигналу. У цих алгоритмах використовується кодування із зворотним зв'язком, коли при передачі сигналу здійснюється оптимізація коду. Закодувавши сигнал, процесор намагається відновити його форму і звіряє результат з початковим сигналом, після чого починає варіювати параметри кодування, домагаючись найкращого збігу. Досягнувши такого збігу, апаратура передає отриманий код по лініях зв'язку; на протилежному кінці відбувається відновлення звукового сигналу. Ясно, що для використання такого методу вимагаються ще серйозніші обчислювальні потужності.

Одним з найпоширеніших різновидів описаного методу кодування являється метод LD - CELP (Low - Delay Code - Excited Linear Prediction). Він дозволяє досягти задовільної якості відтворення при пропускній спроможності 16 кбіт/с. Алгоритм застосовується до послідовності цифр, що отримуються в результаті аналого-цифрового перетворення голосового сигналу з 16-розрядним розширенням. П'ять послідовних цифрових значень кодуються одним 10-бітовим блоком - це і дає ті самі 16 кбіт/с. Для застосування цього методу вимагаються великі обчислювальні потужності; зокрема, в березні 1995 р. ITU прийняв новий стандарт - G.723, який передбачається використовувати при стискуванні мові для організації відеоконференцій по телефонних мережах. Цей стандарт є частиною загальнішого стандарту H.324, що описує підхід до організації таких відеоконференцій. Мета -

організація відеоконференцій з використанням звичайних модемів. Основою G.723 являється метод стискування мови MP - MLQ (Multipulse Maximum Likelihood Quantization). Він дозволяє добитися дуже істотного стискування мови при збереженні досить високої якості звучання. У основі методу лежить описана вище процедура оптимізації; за допомогою різних удосконалень можна стискувати мову до рівня 4,8; 6,4; 7,2 і 8,0 кбіт/с. Структура алгоритму дозволяє на основі програмного забезпечення змінювати міру стискування голосу в ході передачі. Затримка, що вноситься кодуванням, не перевищує 20 мс. Підвищуючи ефективність використання смуги пропускання, механізми стискування мови в той же час можуть привести до погіршення її якості і збільшення затримок.

Далі розглянуті деякі основні кодеки, використовувані в шлюзах IP-телефонії операторського рівня.

Кодек G.711

Рекомендація G.711, затверджена ITU в 1984 р., описує кодек, що використовує ІКМ перетворення аналогового сигналу з точністю 8 біт, тактовою частотою 8 кГц і простою компресією амплітуди сигналу. Швидкість потоку даних на виході перетворювача складає 64 кбіт/с (8 біт * 8 кГц). Для зниження шуму квантування і поліпшення перетворення сигналів з невеликою амплітудою при кодуванні використовується нелінійне квантування по рівню (рис. 3.8) згідно із спеціальним псевдо-логарифмічним законом: А-закон для європейської системи ИКМ-30/32.

Перші ІКМ кодеки з нелінійним квантуванням з'явилися вже в 60-х роках. Кодек G.711 широко поширений в системах традиційної телефонії з комутацією каналів. Не дивлячись на те, що рекомендація G.711 в стандарті H.323 являється основний і первинною, в шлюзах IP-телефонії цей кодек застосовується рідко через високих вимог до смуги пропускання і затримок в каналі передачі (все-таки 64 кбіт/с це багато). Використання G.711 в системах IP-телефонії обґрунтоване лише в тих випадках, коли вимагається забезпечити максимальну якість кодування мовної інформації при невеликому числі одночасних розмов. Одним з прикладів застосування кодека G.711 можуть послужити IP-телефони компанії Cisco.

Кодек G.726

Один із старих алгоритмів стискування мови ADPCM - адаптивна диференціальна ІКМ (стандарт G.726 був прийнятий в 1984 р.). Цей алгоритм дає практично таку ж якість відтворення мови, як і ІКМ, проте для передачі інформації при його використанні вимагається смуга всього в 16-32 кбіт/с. Метод заснований на тому, що в аналоговому сигналі, передаваючому мову, неможливі різкі скачки інтенсивності. Тому, якщо кодувати не саму амплітуду сигналу, а її зміну в порівнянні з попереднім значенням, то можна обійтися меншим числом розрядів. У ADPCM зміна рівня сигналу кодується чотирирозрядним числом, при цьому частота виміру амплітуди сигналу зберігається незмінною. Процес перетворення не вносить істотної затримки і вимагає від DSP 5,5-6,4 MIPS (Million Instructions Per Second). Кодек може застосовуватися спільно з кодеком G.711 для зниження швидкості кодування останнього. Кодек призначений для використання в системах відеоконференцій.

Кодек G.723.1

Рекомендація G.723.1 описує гібридні кодеки, що використовують технологію кодування мовної інформації, скорочено звану - MP - MLQ (Multy - Pulse - Multy Level Quantization - множинне імпульсне, багаторівневе квантування), ці кодеки можна охарактеризувати, як комбінацію АЦП/ЦАП і вокодера. Своїм виникненням гібридні кодеки зобов'язані системам мобільного зв'язку. Застосування вокодера дозволяє понизити швидкість передачі даних в каналі, що принципово важливе для ефективного використання радіотракту і IP -канала. Основний принцип роботи вокодера - синтез початкового мовного сигналу за допомогою адаптивної заміни його гармонійних складових відповідним набором частотних фонем і узгодженими шумовими коефіцієнтами. Кодек G.723 здійснює перетворення аналогового сигналу в потік даних із швидкістю 64 кбіт/с (ІКМ), а потім за допомогою багатосмугового цифрового фільтру/вокодера виділяє частотні фонеми, аналізує їх і передає по IP-каналу інформацію тільки про поточний стан фонем в мовному сигналі. Цей алгоритм перетворення дозволяє понизити швидкість кодованої інформації до 5,3-6,3 кбіт/с без видимого погіршення якості мови. Кодек має

дві швидкості і два варіанти кодування: 6,3 кбіт/с з алгоритмом MP - MLQ і 5,3 кбіт/с з алгоритмом CELP. Перший варіант призначений для мереж з пакетною передачею голосу і забезпечує кращу якість кодування в порівнянні з варіантом CELP, але менш адаптований до використання в мережах із змішаним типом трафіку (голос/дані).

Процес перетворення вимагає від DSP 16,4-16,7 MIPS і вносить затримку 37 мс. Кодек G.723.1 широко застосовується в голосових шлюзах і інших пристроях IP-телефонії. Кодек поступається за якістю кодування мови кодеку G.729a, але менш вимогливий до ресурсів процесора і пропускної спроможності каналу.

Кодеки G.729

Сімейство включає кодеки G.729, G.729 Annex A, G.729 Annex B (містить VAD і генератор комфортного шуму). Кодеки G.729 скорочено називають CS - ACELP Conjugate Structure - Algebraic Code Excited Linear Prediction - зв'язана структура з керованим кодом алгебри лінійним пророцтвом. Процес перетворення використовує DSP 21,5 MIPS і вносить затримку 15 мс. Швидкість кодованого мовного сигналу складає 8 кбіт/с. У пристроях VoIP цей кодек займає лідируюче положення, забезпечуючи найкращу якість кодування мовної інформації при досить високій компресії.

Кодек G.728

Гібридний кодек, описаний в рекомендації G.728 в 1992 р. відноситься до категорії LD - CELP - Low Delay - Code Excited Linear Prediction - кодек з керованим кодом лінійним пророкуванням і малою затримкою. Кодек забезпечує швидкість перетворення 16 кбіт/с, вносить затримку при кодуванні від 3 до 5 мс і для реалізації потрібний процесор з швидкодією більше 40 MIPS. Кодек призначений для використання, в основному, в системах відеоконференцій. У пристроях IP-телефонії цей кодек застосовується досить рідко.