ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

СТОРЧАК К.П., ТКАЛЕНКО О.М., МАРКІНА О.А.

ТЕХНОЛОГІЯ VoIP

НАВЧАЛЬНИЙ ПОСІБНИК

Київ - 2018

УДК 621.395.48
681.327
ББК 32.885

Розглянуто та затверджено
на засіданні кафедри Інформаційних систем та технологій
протокол №10 від 30 квітня 2018 року

Навчальний посібник призначений для студентів денної та заочної форм навчання за спеціальностями 6.050903 Телекомунікації, 172 Телекомунікації та радіотехніка, 126 «Інформаційні системи та технології», а також може бути корисним широкому колу спеціалістів в області телекомунікацій, аспірантам, для інженерів Операторських компаній, науково-дослідних, проектних і виробничих організацій.

Сторчак К.П., Ткаленко О.М., Маркіна О.А. Технологія VoIP. Навч. посібник, підготовлено для студентів вищих навчальних закладів – Київ: ДУТ, 2018. – 120с.

У посібнику розглянуті принципи технології передавання мови по мережам пакетної комутації, що працюють по протоколу IP (Internet Protocol), розглянуто доцільність використання технології встановлення сеансу зв’язку в IP мережах. Розглянуті архітектури системи IP-телефонії, кодеки VoIP, сценарії IP-телефонії. Описані питання сигналізації, принципи протоколу SIP, принципи протоколу RTP, сценарії сеансів зв`язку, управління транспортними шлюзами. Наведено алгоритми встановлення SIP з’єднань, здійснено аналіз практичного використання протоколу SIP. Приведений огляд обладнання для побудови мереж IP-телефонії.

Рецензенти:
Заїка В.Ф. - завідуючий кафедрою Телекомунікаційних систем та мереж Державного університету телекомунікацій, доктор технічних наук, доцент.
Кунах Н.І. – доктор технічних наук, професор Київського коледжу зв’язку.

ЗМІСТ

ПЕРЕДМОВА

Розвиток технології Voice over IP (VoIP) є засобом підвищення продуктивності праці і розвитку бізнесу. Використання технології VoIP дозволяє надавати користувачам нові сервіси та додатки. IP-телефонія вигідна як користувачам так і операторам мереж, і виробникам обладнання, адже системи VoIP надають співробітникам такі нові інструментальні засоби, як системи присутності і миттєвого обміну повідомленнями з партнерами у всьому світі. Доступність високоякісних широкосмугових звукових кодеків, відеоконференц-зв`язок і сумісне використання документів зробили корпоративний зв`язок значно більш ефективним. Сумісні переваги корпоративних систем VoIP істотно підвищують продуктивність працівників, покращуючи їх взаємодію і комунікабельність. Існує декілька підходів до побудови мереж IP-телефонії. Всі вони регламентують управління мультимедіа-викликами та передавання медіа-трафіку в IP-мережах, але при цьому реалізують різні підходи до побудови систем телефонної сигналізації.

Актуальність розвитку рішень з використанням технології Voice over IP (VoIP) невпинно зростає. Розвиток технології VoIP є засобом підвищення продуктивності праці і розвитку бізнесу будь-якої сучасної компанії. Підприємці використовують системи VoIP для об`єднання мереж передавання голосу і даних, а також для ряду нових додатків, які дозволяють підвищити продуктивність. На теперішній час підприємства використовують системи VoIP для покращення корпоративної взаємодії із своїми віддаленими представництвами. Системи VoIP надають співробітникам такі нові інструментальні засоби, як системи присутності і миттєвого обміну повідомленнями з партнерами у всьому світі.

Протокол SIP є перспективним сучасним протоколом для надавання широкого спектру телекомунікаційних послуг. SIP і протоколи, які його супроводжують, створені і розвиваються в межах IETF (Internet Engineering Task Force) – головного органу стандартизації Інтернет. Частина вимог до реалізацій, які побудовані на новій версії протоколу SIP, не підтримує зворотної сумісності з реалізаціями, які виконані по початковій версії.

У майбутньому IP-телефони перестануть бути аналогами звичайних телефонних апаратів. На основі IP-телефонів будуть будуватися CRM-системи нового покоління, створюватися системи корпоративних баз знань, в результаті відбудеться інтеграція всіх інформаційних сервісів - електронної пошти, відеоконференцій та телефонії - в єдину комунікаційну послугу, яка зможе задовольнити комунікаційні потреби корпоративного клієнта будь-якого масштабу - від дрібних і середніх підприємств до великих корпорацій.

1. ТЕХНОЛОГІЯ ПЕРЕДАВАННЯ ГОЛОСОВОЇ ІНФОРМАЦІЇ З ВИКОРИСТАННЯМ ПРОТОКОЛУ IP - Voice over IP (VoIP)

1.1 Принципи пакетного передавання мови

Інформація, яка передається у вигляді електромагнітних сигналів, може представляти собою: голос, дані, відео зображення або будь-яку їх комбінацію, що називається мультимедійною інформацією.

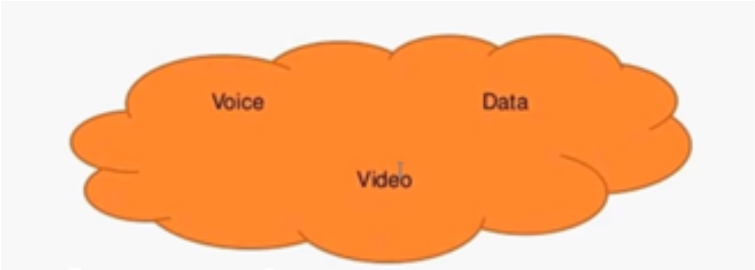

Рис.1. Уніфіковані телекомунікації

Уніфіковані комунікації (Unified Communications — UC) з'явилися в процесі взаємної інтеграції та злиття всіх систем корпоративного обміну інформацією в єдину платформу. Така платформа надає користувачам єдиний зручний інтерфейс, який включається в себе системи IP телефонії, аудіо-, відео- та web-конференцій, обміну поштовими та миттєвими повідомленнями, і модуль виявлення присутності. До недавнього часу всі ці сервіси поставлялися різними вендорами і представляли собою набір незалежних продуктів, пристроїв, а в деяких випадках і окремих мереж, що викликало складнощі при адмініструванні та незручності у використанні таких систем, а також високі операційні витрати. Інтеграція різних типів конференцій відкриває широкі можливості для спілкування, в ході якого можна використовувати текстові, голосові та відеодані. Тепер співробітники отримали можливість організовувати зустрічі з будь-якої точки планети, без необхідності звертатися до незалежних постачальників послуг конференц-зв'язку або збирати всіх в одному місці, отже, це економить час співробітників і зменшує витрати компанії. Переваги уніфікованих телекомунікацій: пропускна спроможність каналів збільшується; інфраструктура для всіх трьох послуг стає безшовною;
впровадження нової послуги або додатка різко скорочується.

На сьогоднішній день успішно реалізована технологія передавання голосової інформації по мережам з маршрутизацією пакетів IP – Voice over IP (VoIP) або IP-телефонія. Поняття «Voice over IP» має на увазі не тільки і не стільки використання мережі Інтернет в якості середовища передавання голосу, скільки

сам протокол IP і технології, що забезпечують надійне та високоякісне передавання голосової інформації у мережах пакетної комутації.

IP-телефонія повинна мати можливість підтримувати спільну роботу та забезпечувати інформаційну прозорість із множиною стандартів зв`язку, які прийняті у різних країнах світу. Мова йде не тільки про електричне стикування – необхідно знайти взаємоприйнятне рішення таких задач, як взаємодія протоколів верхніх рівнів та додатків, нарахування плати та ін.

IP-телефонія забезпечує голосовий зв'язок поверх мереж, що використовують Інтернет-протокол (IP). Технологія дозволяє об'єднати безліч розосереджених об'єктів організації, включаючи мобільних працівників, в єдину конвергентну мережу. IP-телефонія перспективна для компаній, які підтримують інтернет-зв'язок з усіма відділеннями і одночасно платять за використання контурів голосового зв'язку АТС в таких відділеннях. Економія витрат сама по собі є привабливим фактором, а параметри безпеки, надійності і якості зв'язку безсумнівно підштовхнуть менеджерів мереж зробити вибір на користь IP-телефонії.

У технічній літературі використовуються три основних терміни для позначення технології передавання мови по мережам з пакетною комутацією на базі протоколу IP (Internet Protocol): IP-телефонія (IP Telephony); голос по IP-мережам (Voice over IP - VoIP); Інтернет-телефонія (Internet Telephony).

IP-телефонія – технологія, яка використовує мережу з пакетною комутацією повідомлень на базі протоколу IP (наприклад, мережу Інтернет) для передавання голосу в режимі реального часу (в якості засобу організації та ведення міжнародних, міжміських та місцевих телефонних розмов і передавання факсів в режимі реального часу).

За кордоном технологія передавання голосової інформації з використанням протоколу IP має сталу назву Voice over IP (VoIP). Відносно сервісів та технологій між IP-телефонією та VoIP немає ніякої різниці.

Інтернет-телефонія – це приватний випадок IP-телефонії, коли в якості каналів передавання пакетів телефонного трафіку або від абонента до оператора, або на магістралі (або на обох названих ділянках) використовуються звичайні канали мережі Інтернет.

Організатори семінару Міжнародного союзу електрозв'язку (ITU) виступили з пропозицією вважати IP-телефонію загальним поняттям, яке включає Інтернет-телефонію та VoIP. Учасникам семінару було запропоновано для обговорення наступна відмінність технологій:

- *Інтернет-телефонія* – передавання телефонних повідомлень у мережах передавання даних загального користування, тобто у мережах, які мало або не адмініструються;

- *VoIP* – передавання телефонних повідомлень у корпоративних, тобто у мережах, які добре адмініструються.

IP-телефонія є найбільш простою для реалізації послугою із пакету послуг, включаючи передавання даних та відео по протоколу IP.

Архітектура технології Voice over IP може бути спрощено представлена у вигляді двох площин. Нижня площина – це базова мережа з маршрутизацією пакетів IP, верхня площина – це відкрита архітектура управління обслуговуванням викликів (запитів зв`язку) (рис.2).

Програмні засоби управління обслуговуванням викликів	- телефонні системи сигналізації
Базова мережа з маршрутизацією пакетів IP	- RTP/UDP/IP

Рис.2. Рівні архітектури IP-телефонії

Нижня площина представляє собою комбінацію відомих протоколів Інтернет: це – RTP (Real Time Transport Protocol), який функціонує над протоколом UDP (User Datagram Protocol), який розміщений, у свою чергу, у стеку протоколів TCP/IP над протоколом IP. Таким чином, ієрархія RTP/UDP/IP представляє собою свого роду транспортний механізм для голосового трафіку.

Тепер перейдемо до верхньої площини управління обслуговуванням запитів зв`язку. Управління обслуговуванням виклику передбачає прийняття рішення про те, куди виклик повинен бути направлений, і яким чином повинно бути встановлене з`єднання між абонентами. Інструмент такого управління – телефонні системи сигналізації.

Найбільш розповсюдженим є протокол, специфікований у рекомендації H.323. Інший протокол площини управління обслуговуванням виклику – SIP – орієнтований на те, щоб зробити кінцеві пристрої та шлюзи більш інтелектуальними і підтримувати додаткові послуги для користувачів.

У мережах пакетної комутації по каналам зв’язку передаються одиниці інформації, які не залежать від фізичного носія. Такими одиницями можуть бути пакети, кадри або комірки (в залежності від протоколу), але в будь-якому випадку вони передаються по розділяємій мережі (рис.3), більш того – по окремим віртуальним каналам, які не залежать від фізичного середовища. Кожний пакет ідентифікується заголовком, який може містити інформацію про канал, який використовується, його походження (тобто про джерело або відправника) та пункту призначення (про отримувача або приймача).

У мережах на базі протоколу IP всі дані – голос, відео, комп’ютерні програми або інформація у будь-якій іншій формі – передаються у вигляді пакетів. Будь-

який комп’ютер та термінал такої мережі має свою унікальну IP-адресу і пакети, які передаються, маршрутизуються до отримувача у відповідності з цією адресою, яка вказується у заголовку. Дані можуть передаватися одночасно між багатьма користувачами та процесами по одній і тій самій лінії. При виникненні проблем IP-мережі можуть змінювати маршрут для обходу несправних ділянок. При цьому протокол IP не потребує виділеного каналу сигналізації.

Процес передавання голосу по IP-мережі складається із декількох етапів.

На першому етапі здійснюється *оцифровка голосу.* Потім оцифровані дані аналізуються і обробляються з метою зменшення фізичного обсягу даних, які передаються отримувачу. Як правило, на цьому етапі здійснюється подавлення непотрібних пауз та фонового шуму, а також компресування. На наступному етапі отримана послідовність даних розбивається на пакети і до неї добавляється протокольна інформація – адреса отримувача, порядковий номер пакету на випадок, якщо вони будуть доставлені не послідовно, і додаткові дані для корекції помилок. При цьому здійснюється тимчасове накопичення необхідної кількості даних для утворення пакету до його безпосереднього відправлення у мережу.

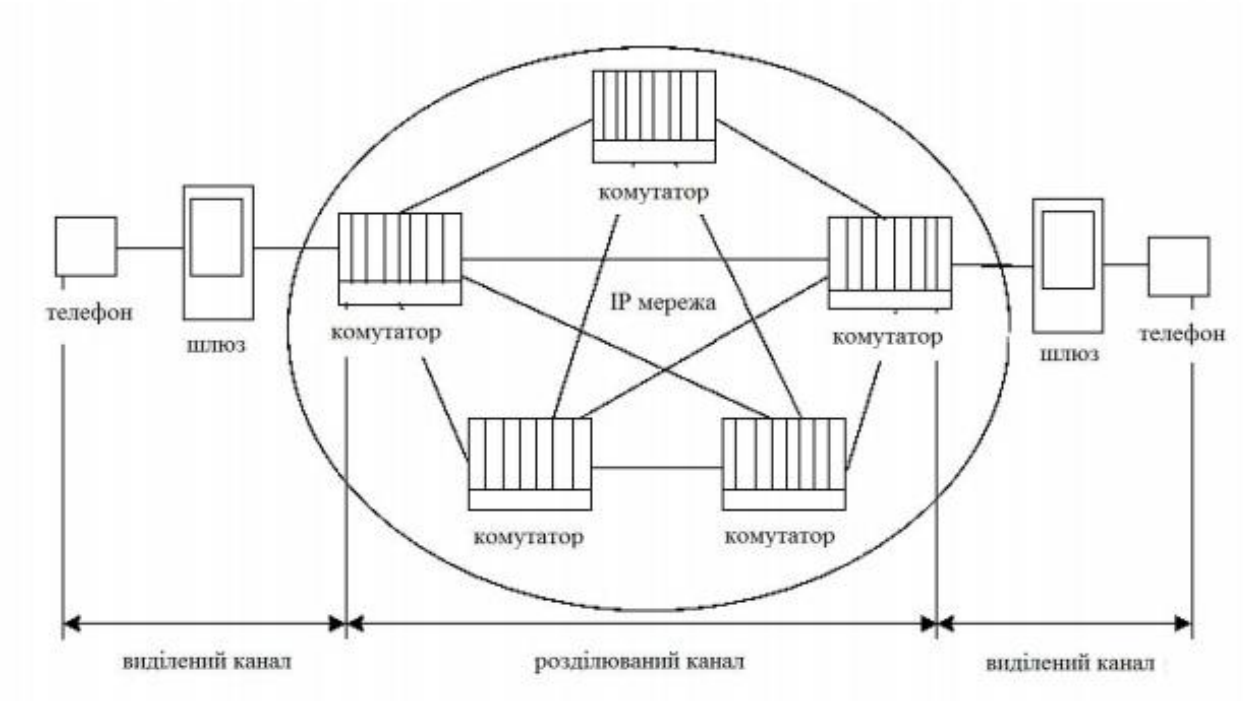

Рис.3. З’єднання в мережі з комутацією пакетів

Витягування переданої голосової інформації із отриманих пакетів також здійснюється в декілька етапів. Коли голосові пакети приходять на термінал отримувача, спочатку перевіряється їх порядкова послідовність. Оскільки IP-мережі не гарантують часу доставки, то пакети із старшими порядковими номерами можуть прийти раніше, більш того, інтервал часу отримання також може коливатися. Для відновлення вихідної послідовності та синхронізації

здійснюється тимчасове накопичення пакетів. Але деякі пакети можуть бути зовсім втрачені при доставці, або затримка їх доставки перевищує допустиме розкидання. У звичайних умовах прийомний термінал запитує повторне передавання помилкових або втрачених даних. Але передавання голосу дуже критичне до часу доставки, тому в цьому випадку або включається алгоритм апроксимації, який дозволяє на основі отриманих пакетів приблизно відновити втрачені, або ці втрати просто ігноруються, а пропуски заповнюються даними випадковим чином.

Отримана таким чином (не відновлена!) послідовність даних декомпресується і перетворюється безпосередньо в аудіо-сигнал, який переносить голосову інформацію користувачу.

Для того, щоб здійснити міжміський (міжнародний) зв'язок за допомогою телефонних серверів, організація або оператор послуги повинен мати по серверу у тих місцях, куди і звідки плануються дзвінки.

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

Для рішень IP-телефонії характерна визначена модульність: кількість і потужність різних вузлів – шлюзів, gatekeeper («привратників» - так у термінології VoIP називаються сервери обробки номерних планів) – можна нарощувати практично незалежно, у відповідності з поточними потребами.

1.2 Види з'єднань у мережі IP-телефонії

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

1. *«Від телефону до телефону»* (рис.4). Виклик надходить із звичайного телефонного апарату до АТС, на один із виходів якої підключений шлюз IP-

телефонії, і через IP-мережу доходить до іншого шлюзу, який здійснює зворотнє перетворення.

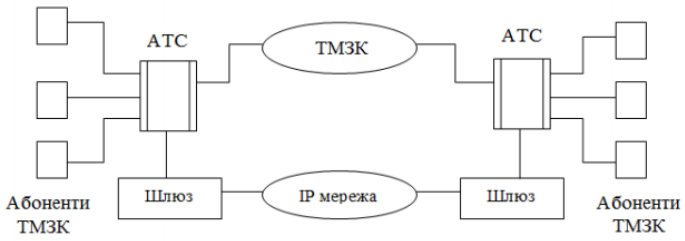

Рис.4. Схема зв'язку «телефон-телефон»

2. «Від комп'ютера до телефону» (рис.5). Мультимедійний комп'ютер, який має програмне забезпечення IP-телефонії, звукову плату (адаптер), мікрофон та акустичні системи, підключається до IP-мережі або до мережі Інтернет, а з іншого боку шлюз IP-телефонії має з'єднання через АТС із звичайним телефонним апаратом. *Звуковий адаптер* – це спеціальний пристрій на ПК, який відповідає за виведення звуку. Звукові карти бувають *зовнішніми* (у вигляді плати адаптера) та *вбудованими* (інтегровані) у материнську плату.

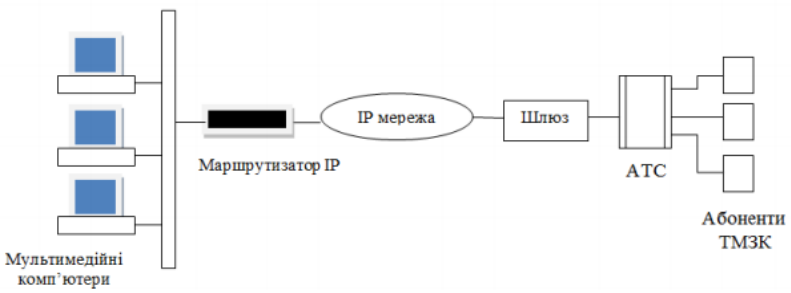

Рис.5. Схема зв'язку «комп'ютер-телефон»

Потрібно зазначити, що у з'єднаннях 1 і 2 видів замість телефонних апаратів можуть бути включені факсимильні апарати, і в цьому випадку мережа IP-телефонії повинна забезпечувати передавання факсимильних повідомлень.

3. «Від комп'ютера до комп'ютера» (рис.6). В цьому випадку з'єднання встановлюється через IP-мережу між двома мультимедійними комп'ютерами, які обладнані апаратними та програмними засобами для роботи з IP-телефонією.

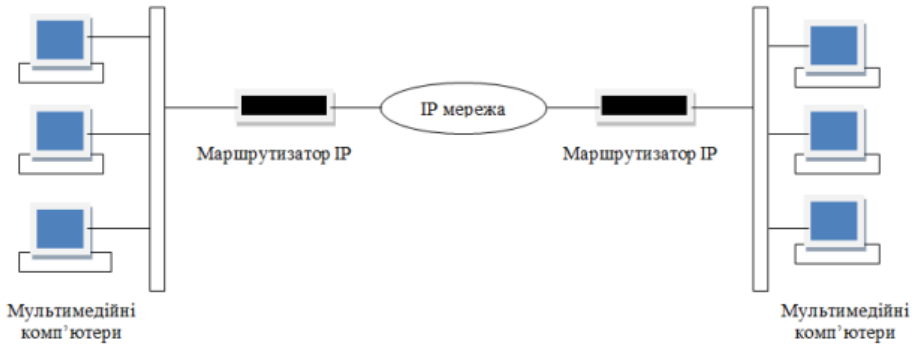

Рис.6. Схема зв'язку «комп'ютер- комп'ютер»

4. «Від WEB браузера до телефону» (рис.7). З розвитком мережі Інтернет став можливий доступ і до голосових послуг. Наприклад, на WEB-сторінці деякої компанії у розділі «Контакти» розміщується кнопка «Виклик», натиснувши на яку можна здійснити голосове з'єднання з представником даної компанії без набору телефонного номеру. Вартість такого дзвінка для викликаючого користувача входить у вартість роботи у мережі Інтернет.

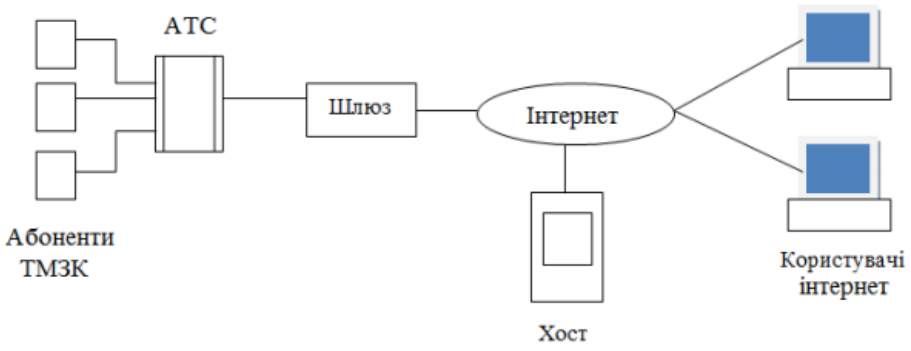

Рис.7. Схема зв'язку «WEB-браузер- телефон»

WEB-телефонія – це процес здійснення дзвінків з використанням тільки браузера хоча б з одного боку.

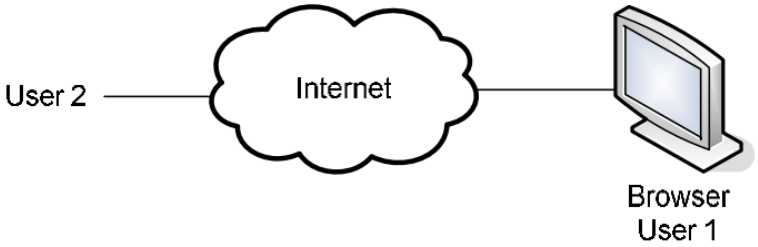

Рис.8

Можливі сценарії WEB-телефонії:

- браузер – телефон (в тому числі SIP-softphone);
- браузер-браузер.

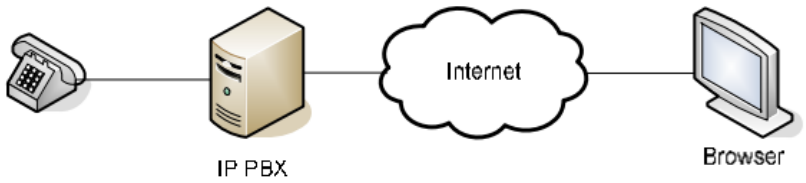

Рис.9. Браузер – телефон

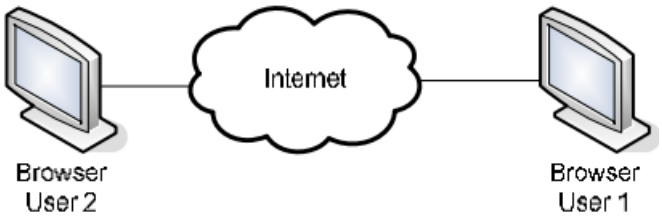

Рис.10. Браузер-браузер

Сценарій WEB-телефонії «браузер-браузер» може здійснюватися *через медіа-сервер* або *peer-to-peer*.

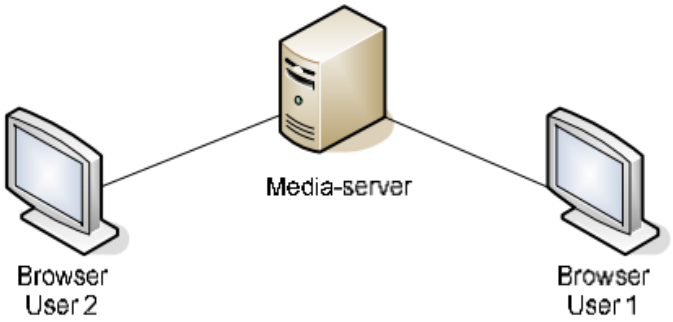

Рис.11. Сценарій WEB-телефонії «браузер-браузер» через медіа-сервер

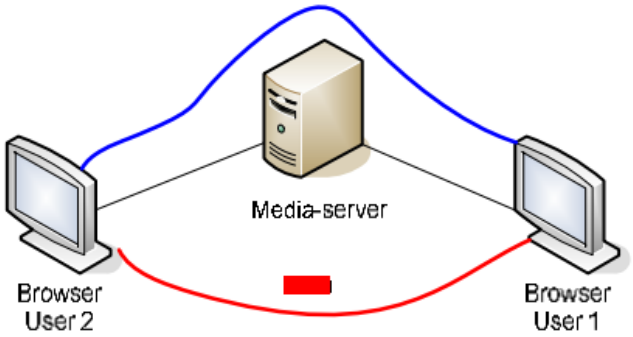

Рис.12. Сценарій WEB-телефонії «peer-to-peer»

Використання медіа-серверу має добру прохідність трафіку (NAT, Firewall). Як недоліки, слід зазначити, навантаження на сервер, великий час відгуку, можливість використовувати тільки протокол TCP.

Перевагами використання p2p є побудова на базі протоколу UDP, гарна якість зв'язку, відсутність навантаження на сервер. Як недоліки, слід зазначити, погану прохідність трафіку через Firewall і NAT, необхідність Flash Player 10 версії.

Для сценарію WEB-телефонії «браузер – телефон» необхідний SIP-шлюз.

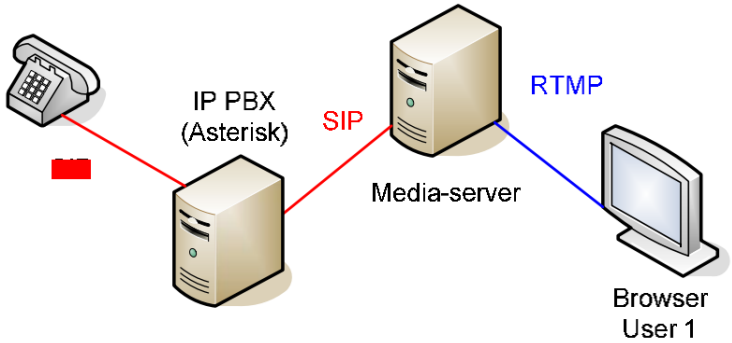

Рис.13. Використання SIP-шлюзу у сценарії WEB-телефонії «браузер – телефон»

Сфери використання: інтернет-магазини; on-line підтримка; корпоративні рішення; рішення для ISP; рекламні сервіси; інтернет-сервіси.

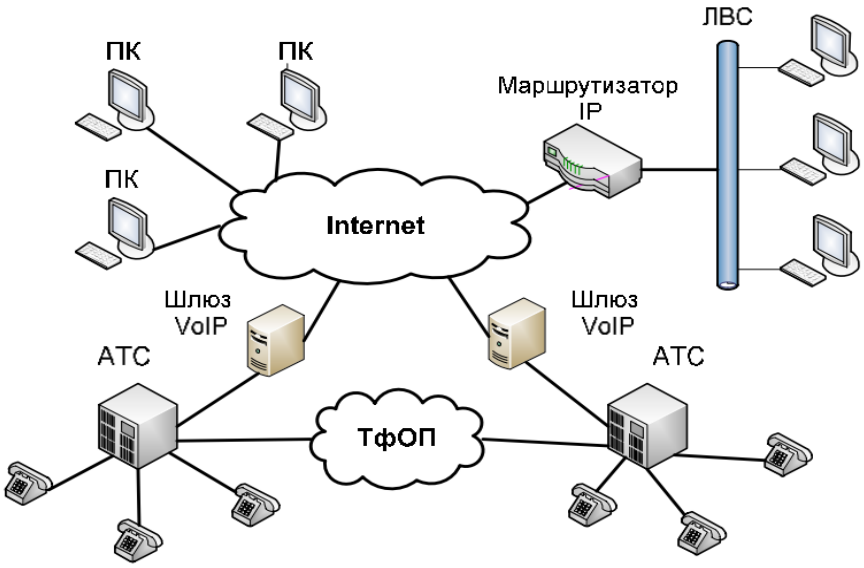

Рис.14. Загальний вигляд мережі IP-телефонії

1.3 Переваги та недоліки використання IP-телефонії

Кінцевий користувач IP-телефонії отримує наступні додаткові переваги:

Більш низькі ціни на послуги телефонного зв'язку. Менші витрати на традиційні телефонні розмови (особливо міжміські і міжнародні). Тобто *зменшення вартості телекомунікацій.* Для організації телефонного зв'язку між офісами компанії по всьому світу достатньо лише мати доступ до мережі Інтернет. Як приклад, можна привести *скайп* – розмовляємо з будь-якою точкою світу, а сплачуємо тільки за сам доступ до мережі Інтернет. Підключення до мережі можливе з будь-якої точки світу, де є Інтернет. Наш телефонний номер зберігається у будь-якій точці світу. Дзвінки тривалістю в 15 секунд, як правило, не тарифікуються. *Зменшення вартості кабельної інфраструктури*. VoIP дозволяє впровадити телефонію на вже існуючій СКС. Є Ethernet-розетки, кабелі – вже поверх цього ми можемо включити і організувати IP-телефонію, при цьому не збільшуючи загальну кількість портів, яка виділена для нашого кінцевого обладнання. В результаті, набагато менші витрати на інвестиції в обладнання. *Вища ефективність використання існуючих телефонних ліній* (передавання більше одного телефонного дзвінка в межах високошвидкісного телефонного підключення). Під час розмови голосові сигнали перетворюються у пакети даних, які потім стискаються. Далі ці пакети даних надсилаються через Інтернет прийомній стороні. Коли пакети даних досягають адресата, вони декодуються в аналоговий голосовий сигнал. Маємо достатню пропускну спроможність, а коштує це досить недорого. *Підтримка голосу та даних.* Додаткові можливості поєднаного доступу до мережі Інтернет (голосова інформація та дані можуть

передаватися по одній і тій самій мережі). *Незалежність від місцярозташування.* Мобільність користувача, так як дзвінки та факси автоматично перенаправляються у будь-яку точку світу. Така розподілена архітектура забезпечує гнучкість та робить можливим відсутність прив'язки до місця надання послуги. *Новий набір пристроїв доступу. Додаткові телефонні властивості.* Доступ до нових послуг (голосова пошта, конференцзв'язок, переадресація дзвінка, передавання факсу та ін.) через відкритий інтерфейс архітектури на базі IP, що забезпечує сумісність для широкого спектру розробників додатків. Можливість переадресації викликів по IP-мережі. *Можливість налаштування набору послуг. Простота оплати послуг IP-телефонії. Простота контролю користувачем стану його розрахункового рахунку* (через мережу Інтернет). *Безшовні голосові мережі.* Середовище доступу уніфіковане: тобто, якщо ми встановлюємо на свій ПК софтфон (програмний софтфон), скачуємо додаток на телефон або планшет, або користуємося фізичним телефоном, апаратним IP-телефоном – *ми не повинні бути обмежені у плані надання сервісів, вибираючи той чи інший тип додатків.* Тобто це надавання однакового сервісу до будь-яких кінцевих пристроїв. Для всіх абонентів надається однаковий рівень обслуговування і доступ до сервісів. *Централізований контроль.* Управління всіма голосовими пристроями в мережі та маршрутизацією з єдиної точки управління. На маршрутизатор покладається функція по забезпеченню IP-телефонії. В залежності від того, як проходить виклик, ми можемо збирати всю звітність про складання викликів (хто й куди телефонував, скільки розмовляв). Тобто функції білінгу ми можемо централізовано отримати на нашому маршрутизаторі. Можливість організації дзвінків в межах корпоративної мережі (середньої, великої), наприклад, між офісами в Києві та Житомирі через внутрішнє VPN-з'єднання, яке забезпечує безпеку, дозволяє досягати внутрішніх ресурсів в наших віддалених офісах. Це внутрішня телефонія.

Спочатку підприємці використовували системи VoIP для об'єднання своїх мереж передавання голосу та даних. Оскільки об'єднана мережа обходилася дешевше, підприємці почали використовувати її для ряду нових додатків, які дозволяють підвищити продуктивність. На теперішній час підприємці використовують системи VoIP для покращення корпоративної взаємодії із своїми віддаленими представництвами. Системи VoIP надають співробітникам такі нові інструментальні засоби, як системи присутності та миттєвого обміну повідомленнями з партнерами у всьому світі. Доступність високоякісних широкосмугових звукових кодеків, відеоконференц-зв'язок та сумісне використання документів зробили корпоративний зв'язок значно більш ефективним. Сумісні переваги корпоративних систем VoIP суттєво підвищують продуктивність службовців, покращуючи їх взаємодію та комунікабельність.

2. АРХІТЕКТУРИ СИСТЕМ IP-ТЕЛЕФОНІЇ

2.1 Архітектура системи на базі стандарту H.323

Для забезпечення сумісності кінцевого обладнання і шлюзів різних виробників проблемами стандартизації IP-телефонії займаються декілька міжнародних організацій: Сектор стандартизації телекомунікацій Міжнародного союзу електрозв`язку МСЕ-Т (International Telecommunications Union – Telecommunications, ITU-T); Європейський інститут стандартизації по телекомунікаціям (European Telecommunication Standard Institute, ETSI); Робоча група по інженерним проблемам Інтернет (Internet Engineering Task Force - IETF); Американський національний інститут стандартів (American National Standards Institute, ANSI); Інститут інженерів з електротехніки та електроніки (Institute of Electrical and Electronics Engineers, IEEE); Форум VoIP (Voice over IP).

Для передавання мовної інформації через IP-мережу Рекомендація H.323 обов'язкова, тобто фактично є стандартом. Набір рекомендацій МСЕ-Т H.323 визначає мережні компоненти, протоколи і процедури, які дозволяють організувати мультимедіа-зв'язок у пакетних мережах, у тому числі в ЛОМ Ethernet. Вони визначають порядок функціонування абонентських терміналів у мережах з розділяємим ресурсом. H.323-сумісні пристрої можуть застосовуватися для телефонного зв'язку (IP-телефонія), передавання звуку та відео (відеотелефонія), а також звуку, відео та даних (мультимедійні конференції).

Основною метою розробки стандарту H.323 стало забезпечення взаємодії з іншими типами мереж мультимедіа-зв'язку (рис.15). Це завдання реалізується за допомогою *шлюзів,* які здійснюють трансляцію сигналізації та форматів даних. При умові відповідності стандарту пристрої з різними можливостями можуть і взаємодіяти один з одним. Стандарт H.323 визначає також порядок взаємодії з кінцевими пристроями інших стандартів.

Рекомендації H.323 передбачають: управління смугою пропускання; можливість взаємодії мереж; платформенну незалежність; підтримку багатоточкових конференцій; підтримку багатоадресного передавання; стандарти для кодеків; підтримку групової адресації.

Термінали H.323 можуть бути інтегровані у персональні комп'ютери або реалізовані як автономні пристрої. Підтримка мовного обміну – обов'язкова функція для пристрою стандарту H.323. У рекомендації H.323 описуються чотири основні компоненти VoIP-з'єднання (рис.16): термінал; gatekeeper (контролер зони); шлюз; пристрій управління багатоточковою конференцією (MCU).

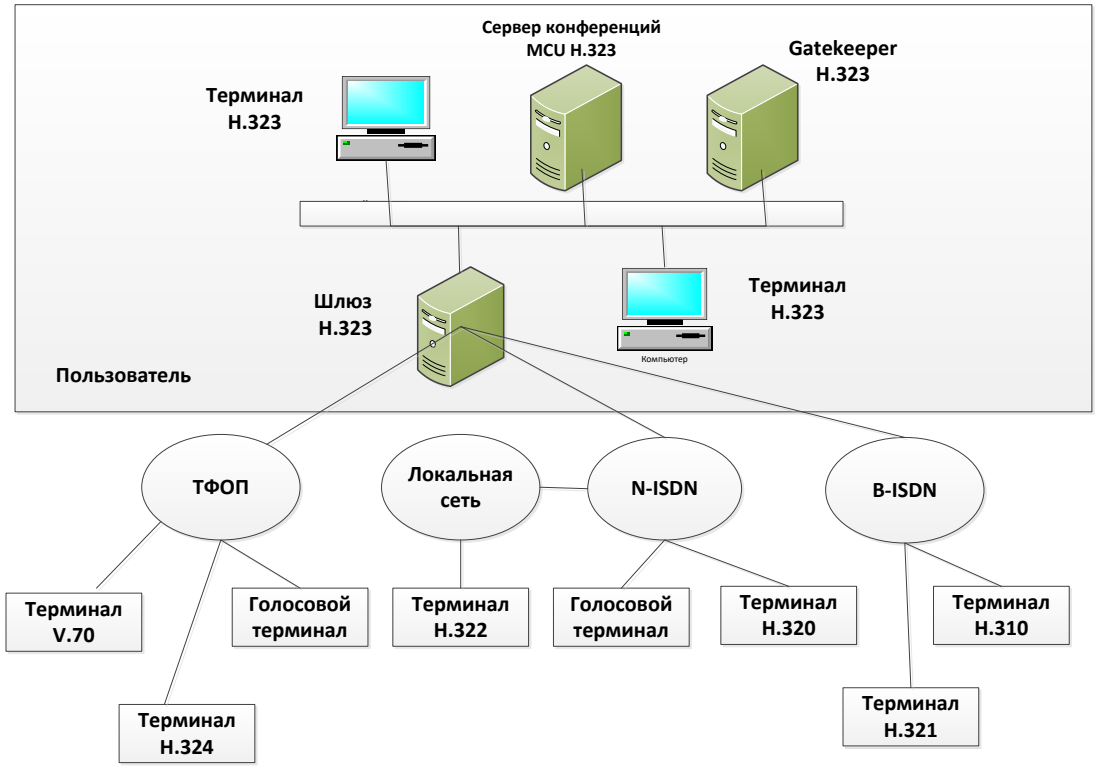

Рис.15. Конфігурація мережі на базі стандарту H.323

Табл.1. Основні компоненти стандарту H.323

Рекомендація	**Опис**
H.225	Визначає повідомлення по управлінню викликом, включаючи сигналізацію і реєстрацію, а також пакетизацію і синхронізацію потоків мультимедійних даних
H.245	Визначає повідомлення для відкриття і закриття каналів для передавання потоків мультимедійних даних, а також інші команди та запити
H.261	Відеокодек для аудіовізуальних сервісів на каналах P x 64 кбіт/с
H.263	Описує новий відеокодек для передавання відео по звичайним телефонним мережам
G.711	Аудіо кодек, 3,1 кГц на 48, 56 і 64 кбіт/с
G.722	Аудіо кодек, 7 кГц на 48, 56 і 64 кбіт/с
G.728	Аудіо кодек, 3,1 кГц на 16 кбіт/с
G.723	Аудіо кодек, для режимів 5,3 і 6,3 кбіт/с
G.729	Аудіо кодек

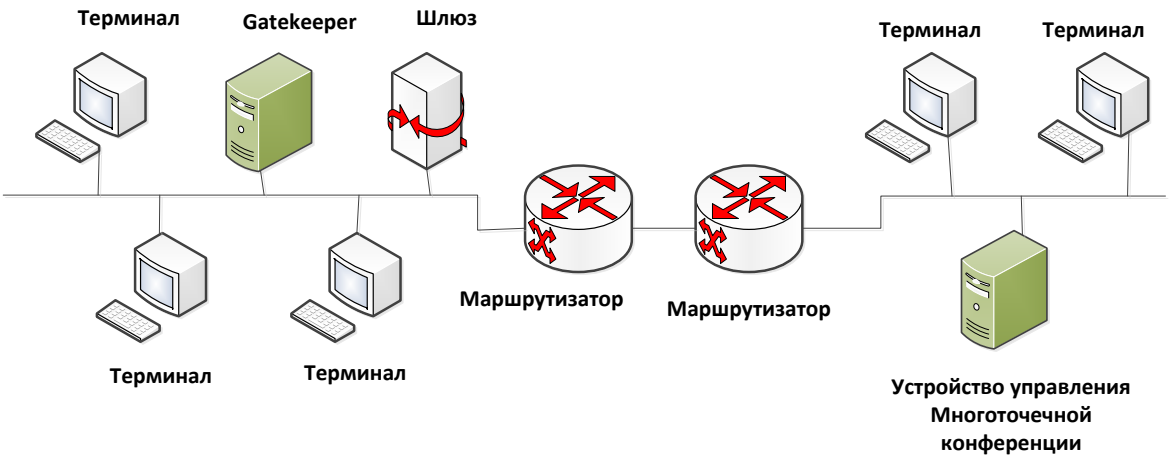

Рис.16. Зона H.323

Всі перераховані компоненти організовані в *зони H.323*. Одна зона складається із gatekeeper та декількох кінцевих точок, причому gatekeeper управляє всіма кінцевими точками своєї зони. Зоною може бути і вся мережа постачальника послуг IP-телефонії або її частина, яка охоплює окремий регіон. Поділ на зони H.323 не залежить від топології пакетної мережі.

Термінал H.323 представляє собою кінцеву точку в мережі, яка здатна передавати та приймати трафік у масштабі реального часу, взаємодіючи з іншими терміналом H.323, шлюзом або пристроєм управління багатоточковою конференцією (MCU). Для забезпечення цих функцій термінал включає: елементи аудіо (мікрофон, акустичні системи, телефонний мікшер, система акустичного ехоподавлення); елементи відео (монітор, відеокамера); елементи мережного інтерфейсу; інтерфейс користувача.

H.323-термінал повинен підтримувати протоколи H.245, Q.931, RAS, RTP/RTCP та сімейство протоколів H.450, а також включати в себе аудіокодек G.711. *H.245* для встановлення можливостей терміналів і створення каналу обміну аудіоінформацією. *H.225* для сигналізації виклику та встановлення параметрів зв'язку. *RAS* для реєстрації терміналу користувача та встановлення додаткових параметрів управління контролером зони. *RTP/RTCP* для впорядкування звукових та відеопакетів.

Прикладом терміналу, який підтримує стандарт H.323, є апарат фірми Selsius Systems (компанії Cisco Systems) – цифровий системний телефон, який об-лаштований інтерфейсом Ethernet замість порту RJ-11. Такий термінал, використовуючи власні процесори, мікропрограмні кодеки та стек TCP/IP, забезпечує високу якість звуку та рівень надійності.

Протоколи *H.225* та *RAS* використовуються між H.323 кінцевими точками (терміналами та шлюзами) і контролером зони для забезпечення: виявлення контролеру зони (GRQ); реєстрації кінцевої точки; визначення розміщення

кінцевої точки; управління аутентифікацією; завдання маркеру доступу.

RAS-повідомлення передаються через ненадійні RAS-канали, тому при обміні повідомленнями можливі втрати, затримки та повторне передавання.

Шлюз забезпечує перетворення двонаправленої аналогової мови у цифрову форму всередині кодуючого/декодуючого пристрою (кодеку); стиснення інформації (голосу), конвертування її (його) в IP-пакети та направлення в IP-мережу (упаковка цифрових даних в пакети для передавання по IP-мережі). З протилежного боку шлюз здійснює зворотні дії: розшифровку та розформування пакетів викликів. В результаті звичайні телефонні апарати без проблем приймають ці виклики.

Таке перетворення інформації не повинне значно спотворити вихідний мовний сигнал, а режим передавання зобов'язаний зберегти обмін інформацією між абонентами реальному масштабі часу.

Функції шлюзу: реалізація фізичного інтерфейсу з телефонною та IP-мережею; детектування та генерація сигналів абонентської сигналізації; перетворення сигналів абонентської сигналізації у пакети даних і навпаки; перетворення мовного сигналу у пакети даних та навпаки; з'єднання абонентів;
передавання по мережі сигналізаційних та мовних пакетів; роз'єднання зв'язку.

Задачі управління та зв'язку здійснюються за допомогою *універсального процесора*, а задачі сигнальної обробки та телефонного інтерфейсу здійснюються на *цифровому процесорі обробки сигналів*.

Рис.17. Шлюзи

Схема обробки сигналів у шлюзі при підключенні аналогового двухпроводного телефонного каналу PSTN показана на рис.18.

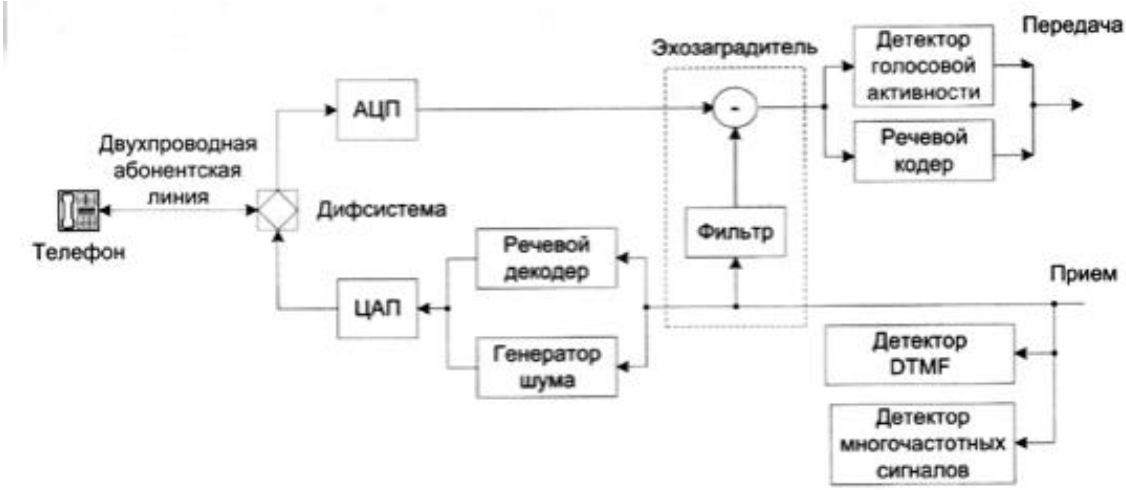

Рис.18. Схема обробки сигналів у шлюзі

Телефонний сигнал з двохпровідної АЛ надходить на диференціальну систему, яка розділяє приймальну і передавальну частини каналу. Далі сигнал передавання разом з частиною сигналу прийому (тією, яка «просочилася») подається на аналого-цифровий перетворювач (АЦП) і перетворюється у 8-мирозрядний кодовий сигнал. У пристрої ехо-компенсації (Echo canceller) із сигналу передавання видаляються залишки приймаємого сигналу. Ехокомпенсатор представляє собою цифровий фільтр, який обробляє цифровий сигнал з метою виділення і/або подавлення визначених частот цього сигналу. Для виявлення і визначення сигналів внутрішньо смугової багато частотної телефонної сигналізації (MF сигналів), сигналів частотного (DTMF) або імпульсного наборів використовуються детектори відповідних типів. Подальша обробка вхідного сигналу здійснюється у голосовому (мовному) кодері (Speech Coder). В аналізаторі кодеру сигнал сегментується на окремі фрагменти певної тривалості (в залежності від методу кодування) і кожному вхідному блоку ставиться у відповідність спектральний інформаційний кадр відповідної довжини.

Частина параметрів, яка обчислена в аналізаторі кодеру, використовується у блоці визначення голосової активності (VAD – voice activity detector), який вирішує, чи є поточний аналізуємий фрагмент сигналу мовою або паузою. При наявності паузи інформаційний кадр може не передаватися у службу віртуального каналу. На прийомному боці із віртуального каналу в логічний надходить або інформаційний кадр, або прапор наявності паузи. На паузних кадрах замість голосового синтезатору включається генератор комфортного шуму (Noise Generator), який відновлює спектральний склад паузного сигналу.

Наявність інформаційного кадру (а не паузи) включає мовний декодер, на виході якого формується мовний сигнал. Для ехокомпенсатора цей сигнал

являється сигналом викликаємого абонента (абонента Б).

Gatekeeper (контролер зони) – виконує функцію управління викликами, виконує роль віртуальної телефонної станції. Gatekeeper виконує наступні функції:

- перетворює адреси псевдоніми у транспортні адреси;
- контролює доступ у мережу на основі авторизації викликів, наявності необхідної для зв'язку смуги частот та інших критерії, що визначені виробником;
- контролює смугу пропускання, управляє шириною смуги пропускання у відповідності з протоколом RAS;
- управляє зонами;
- забезпечує маршрутизацію сигналів виклику.

Gatekeeper здійснює перераховані функції відносно терміналів, шлюзів та пристроїв управління, які зареєстровані на ньому. Ідентифікація вузла може здійснюватися по його поточній IP-адресі, телефонному номеру E.164 або імені – рядку символів на зразок адреси електронної пошти.

Функції gatekeeper можуть бути вбудованими у шлюзи, елементи УВАТС, блоки управління багато точковими конференціями, а також у кінцеві вузли H.323 (термінали). За допомогою механізмів RAS (Registration/Admissions/Status) термінали можуть знаходити gatekeeper та реєструватися в них.

Сервер управління конференціями (MCU – Multipoint Control Union) забезпечує зв'язок трьох та більше H.323-терміналів. Всі термінали, які приймають участь у конференції, встановлюють з'єднання з MCU. Сервер управляє ресурсами конференції, узгоджує можливості терміналів по обробці звуку та відео, визначає аудіо- та відео потоки, які необхідно направляти по багатьом адресам.

По архітектурі MCU поділяються на системи на основі стандартних серверів (Windows NT) та автономні програмно-апаратні комплекси,які встановлюються у стійку.

2.2 Характеристики шлюзів IP-телефонії. Класифікація шлюзів IP-телефонії

У загальному випадку IP-телефонія базується на двух основних принципах: перетворення двонаправленої аналогової мови у цифрову форму всередині кодуючого/декодуючого пристрою (кодека) та упаковку у пакети для передавання по IP. Найчастіше ці функції виконують автономні шлюзові пристрої, які мають декілька різновидів. Це можуть бути виділені пристрої або поєднані маршрутизатори/комутатори із вбудованим апаратним або програмним

забезпеченням шлюзу. Положення шлюзів в мережі IP-телефонії показане на рис.19. Незалежно від способу апаратної реалізації шлюзи IP-телефонії можуть мати ряд характеристик, які приведені нижче.

Сумісність із стандартом H.323

Коли виклики можуть бути направлені на підтримуючі H.323 шлюзи інших виробників.

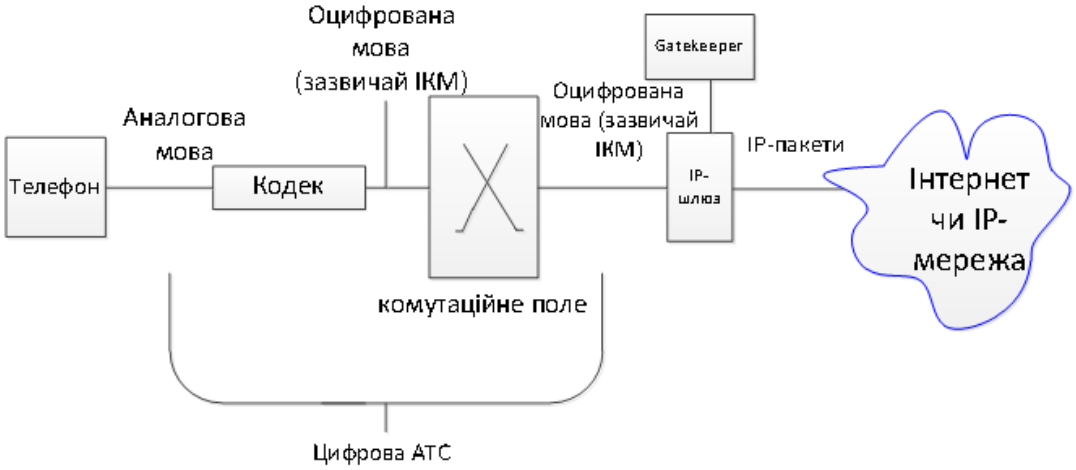

Рис.19. Положення шлюзу в мережі IP-телефонії

Наявність механізмів резервування ресурсів

Підтримка схеми пріоритезації (протокол резервування RSVP або байт диференціації послуг – DS byte) для здійснення можливості вибору пріоритету між передаваємою мовою або даними є важливою харакетристикою шлюзу. При цьому протокол RSVP дозволяє маршрутизаторам притримувати частину смуги пропускання для організації голосового трафіку.

Підтримка основних телефонних інтерфейсів і видів сигналізацій

Важливими критеріями при оцінці характеристик шлюзів є великий різновид телефонних інтерфейсів, які підтримуються IP-шлюзом (E1, PRI, BRI), а також підтримка основних видів телефонної сигналізації: CAS, PRI, ЗКС №7.

Транспортні архітектури

Діапазон транспортних архітектур, з якими працюють сучасні шлюзи, досить широкий: виділені лінії, ISDN, Frame Relay, ATM, Ethernet.

Масштабованість

Важливою характеристикою шлюзу є його масштабованість, що забезпечується модульною побудовою обладнання. На першому етапі розгортання

мережі IP-телефонії можливе використання неповного ресурсу наявних портів при поступовому подальшому збільшенні кількості задіяних голосових портів. При цьому кількість портів відповідає кількості одночасних викликів, які може зробити шлюз, оскільки кожний його порт облаштований власним цифровим сигнальним процесором DSP (Digital Signal Processor) для оцифровки голосових сигналів.

Управління шлюзом

Шлюзи можуть відрізнятися передбаченими засобами управління. Дані засоби управління мають функцію маршрутизації викликів між шлюзами та перекодування телефонних номерів в IP-адреси. Такими засобами облаштовуються майже всі шлюзи. Вони конструктивно можуть бути інтегровані із шлюзом або представляти собою окремий мультимедійний менеджер конференцій або багатоголосовий менеджер доступу. Одним із рішень є використання єдиного пакету, який включає в себе засоби білінгу, маршрутизації викликів та мережного адміністрування.

Можливість встановлення різних алгоритмів кодування мови

На показники якості передаваємого голосу по IP-мережі суттєво впливає схема кодування, яка використовується у шлюзі VoIP при стисканні голосової інформації. Найбільш розповсюджена схема, яка забезпечує найбільшу ступінь стиснення інформації і відповідає специфікації G.723.1 (до 5,3 кбіт/с). Використовуються й інші схеми - G.729a G.711, G.726, G.728. При цьому надзвичайно важливим є облаштування шлюзу додатковою установкою схеми стиснення голосу, яка використовується. Для різних задач і при різних умовах власник має можливість визначити для роботи шлюзу той або інший алгоритм кодування.

Шлюзи IP-телефонії по масштабності застосування можна розділити на два основних види: *шлюзи, орієнтовані на корпоративне застосування; шлюзи, призначені для операторів та постачальників послуг зв'язку.* Продукти останнього виду відрізняються більшою ємністю і масштабованістю, наявністю засобів аутентифікації та моніторингу, а також додаткових можливостей білінгу. Типова інсталяція цих шлюзів передбачає їх підключення з одного боку до IP-мережі (наприклад, через Ethernet-інтерфейс), а з іншого – до традиційної ТМЗК (зазвичай по E1-каналам).

Виконання шлюзів IP-телефонії

1. Автономні IP-шлюзи

Складаються із серверів на базі ПК з комплектом голосових плат. Голосові плати не призначені для компресії/декомпресії звуку, тому дана операція

виконується головним процесором ПК. Існують шлюзи на базі ПК-серверів з платами з цифровою обробкою сигналів (Digital Signal Processing - DSP). Автономні пристрої є хорошим рішенням для мереж, які вже мають маршрутизатори від різних виробників. Плати-маршрутизатори, у свою чергу, застосовуються для додаткового облаштування діючого обладнання функціями IP-телефонії.

2. Маршрутизатори-шлюзи

Великі компанії традиційне мережне обладнання облаштовують вузлами, які відповідають за IP-телефонію. Однією з перших у цьому напрямку стала працювати компанія Cisco Systems (пристрої серії 2600 і 3600), яку наслідували інші фірми. Ця продукція – маршрутизатори і пристрої доступу до розподілених мереж із вбудованими шлюзами IP-телефонії – займає окрему, важливу комірку на ринку мережного обладнання.

3. RAS-шлюзи

Складаються із плат, що встановлюються у сервери дистанційного доступу (RAS). Встановлення пристроїв даного типу при побудові IP-мереж виправдане при роботі з додатками з множиною голосових портів, маючи гранично важливе значення.

4. Шлюзи-модулі для УВАТС

Представляють собою конструктивно модулі для класичних установчих АТС. Причому, така система перед тим, як встановити з'єднання через IP-мережу, перевіряє якість зв'язку. У випадку достатньої його якості (норма встановлюється адміністратором системи), з'єднання встановлюється. У протилежному випадку, виклик направляється по традиційним лініям зв'язку. Таким чином, маємо прагнення фірм-виробників поступово замінювати транспортне середовище, не зачіпаючи при цьому телефонний сервіс, що надається кінцевим користувачам.

5. Шлюзи з інтеграцією бізнес-додатків

У міру розвитку систем IP-телефонії провідне місце займають сервіс-функції. При цьому обладнання повинне орієнтуватися не лише на інтеграцію трафіку, але й на інтеграцію бізнес-додатків, яка дозволяє підвищити продуктивність роботи підприємств. Такі системи повинні забезпечувати інтеграцію Web-служб і центрів з обробки викликів. Вона дозволяє реалізувати службу «клацни та говори» для встановлення телефонного зв'язку між відвідувачами Web-вузла компанії та її співробітниками.

6. Установчі АТС на базі шлюзів

Ще один напрямок розвитку обладнання IP-телефонії – побудова установчих телефонних систем на базі інфраструктур ЛОМ.

У випадку, коли недоцільне встановлення окремого серверу для перетворення телефонних сигналів в IP-пакети, використовуються мережні пристрої, які підключаються напряму до мережі 10 Base-T (по типу концентраторів Ethernet). При цьому кожний концентратор представляє, по суті, невелику УАТС з голосовою поштою та автоматичним секретарем, що підключається через роз'єм RJ-14 до зовнішніх і внутрішніх телефонних ліній і через з'єднувачі RJ-45 до локальної мережі Ethernet.

Така система має простоту управління і наявність вбудованих засобів комп'ютерно-телефонної інтеграції. Наприклад, повнофункціональна міні-АТС IPX-1000 представляє собою єдину платформу як для голосового, так і для мережного зв'язку. IPX-1000 – недороге обладнання для невеликого офісу. IPX-1000 надає 2 зовнішніх лінії (FXO інтерфейс, що називається зовнішньою лінією) і 4 паралельних лінії (FXS інтерфейс, що називається внутрішньою лінією). Всі телефонні порти аналогові без яких-небудь технічних обмежень з'єднань. Більш того, IPX-1000 звичайні телефонні функції реалізовані над POTS (Простий Старий Телефонний Сервіс) проводовою інфраструктурою.

IPX-1000 не використовує мережне підключення для виконання звичайних телефонних функцій, таким чином, не впливаючи на роботу мережі. VoIP функції органічно інтегровані у звичайні телефонні функції IPX-1000. Єдиний інтерфейс користувача представляє як звичайні, так і VoIP функції. Крім того, IPX-1000 виконує функції маршрутизатора, IP розділення (NAT), міжмережний фільтр, DHCP сервер і QoS підтримку.

7. Мережні плати з функціями телефонії

Невеликі або великі пристрої, які обладнані портами RJ-11 для підключення звичайного телефонного апарату.

8. Автономні IP-телефони

Представляють собою рішення «все в одному» для однієї лінії. За зовнішнім виглядом і базовим сервісним можливостям апаратні реалізації IP-телефонів особливо не відрізняються від звичайних телефонів, але їх електронна «начинка» дозволяє суттєво зменшити навантаження на персонал, який відповідає за телефонний зв'язок. Такий вид продуктів пропонує компанія Cisco Systems.

Крім апаратної існують і програмні реалізації IP-телефонів. У цьому випадку ПК, який об лаштований гарнітурою або мікрофоном та акустичними системами, перетворюється у багатофункціональний комунікаційний центр. Користувач ПК,

крім доступу до звичайного телефонного сервісу, отримує набір додаткових можливостей: отримання інформації про клієнта, який телефонує (завдяки наявності стандартного інтерфейсу TAPI до інших програм), контроль за телефонними викликами та роботою з голосовою поштою.

2.3 Архітектура системи на базі проекту TIPHON

Європейський інститут стандартизації телекомунікацій ETSI розробив проект, який отримав назву **TIPHON** (Telecommunications and IP Harmonization over Network). Мета проекту – визначення глобальних стандартів на Інтернет-телефонію, які забезпечують взаємодію IP-мереж з телефонними мережами загального користування, а також мережами мобільного зв'язку. При цьому для доступу абонентів PSTN до користувачів послуг IP-телефонії пропонується виділити глобальний код служби у міжнародному плані нумерації, що визначений у Рекомендації ITU-T E.164.

Функціональна модель TIPHON також складається з трьох компонентів: gatekeeper; шлюз; термінал. Але шлюз розділений на три функціональних об'єкти. Це шлюз сигналізації (SG); транспортний шлюз (MG); контролер транспортного шлюзу (MGC).

SG служить проміжною ланкою сигналізації між мережами IP та мережами на основі комутації каналів. До задач транспортного шлюзу входять:

- перетворення і/або перекодування інформації, що передається;
- забезпечення термінування ІКМ-трафіку, МКК (мереж на основі комутації каналів) і пакетного трафіку. *Термінація трафіку* - це встановлення, підтримка фізичного і/або логічного з'єднання, пропускання трафіку між телекомунікаційною мережею, з якої надходить виклик або ініціюється з'єднання, і кінцевим обладнанням, до якого направляється виклик або ініціюється з'єднання;
- трансляція адрес. *Трансляція мережних адрес* - це технологія, яка дозволяє використовувати для внутрішньої мережі будь-які адреси;
- ехоподавлення – термін, який використовується в телефонії і представляє собою процес видалення відлуння із звуків, що передаються, для підвищення якості передавання голосу по телефону;
- відтворення різних повідомлень для абонентів;
- прийом та передавання цифр кодом DTMF.

Основна функція **MG** – перетворення ІКМ-трафіку у IP-пакети і навпаки. В якості цього елементу можуть використовуватися різні пристрої:

- шлюзи;
- сервери доступу;
- системи передавання АТМ;

- сервери інтерактивних голосових повідомлень.

MGC виконує процедури сигналізації H.323 і перетворює повідомлення сигналізації мереж з комутацією каналів у повідомлення сигналізації H.323. Основна його задача – управляти роботою транспортного шлюзу, тобто здійснювати контроль за з'єднаннями, використанням ресурсів, трансляцій протоколів.

Змодельований на основі трьох описаних елементів шлюз сприймається зовнішніми елементами як єдина система. Причому ці три елементи можуть не бути фізично розділені, але таке розділення дає визначені переваги.

Рішення з трьома шлюзами дозволяє обробляти більшу кількість викликів, так як при цьому функції розділені по окремим процесорам.

Gatekeeper відповідає за контроль та управління об'єктами мережі: виконує перетворення адрес (наприклад, телефонних номерів у відповідні IP-адреси H.323 і навпаки) та маршрутизацію викликів.

Gatekeeper у моделі TIPHON підтримує всі ті ж функції, які визначені для нього у стандарті H.323. Але gatekeeper також відповідає за:

- тарифікацію;
- взаєморозрахунки;
- складання звітів по використанню ресурсів;
- управління.

Розроблена в межах проекту TIPHON модель мережі, яка складається із функціональних елементів та інтерфейсів між ними, показана на рис.20.

Щоб відповідати рекомендаціям TIPHON, продукти повинні підтримувати наступні інтерфейси:

- інтерфейс D – призначений для маршрутизації викликів між контролерами зони (gatekeeper);
- інтерфейс C – для взаємодії між шлюзом MGC та контролером зони;
- інтерфейс N – визначає особливості взаємодії між об`єктами MGC та MG.

Контролер і шлюз обмінюються інформацією при:

- створенні, модифікації та розриві з'єднань;
- визначенні потрібного формату інформації;
- включенні у потік тональних сигналів (тональний набір, тональний сигнал (англ. Dual-Tone Multi-Frequency, DTMF) - двохтональний багаточастотний аналоговий сигнал, який використовується для набору телефонного номера. По смузі частот, яка використовується, сигнал відповідає телефонії) і різних голосових повідомлень;
- запиті відповідей по подіям, які пов'язані із проходженням інформаційного потоку.

Показані на рис.20 служби підтримки можуть бути використані для

аутентифікації, білінгу (*білінг* в електрозв'язку - комплекс процесів і рішень на підприємствах зв'язку, відповідальних за збір інформації про використання телекомунікаційних послуг, їх тарифікацію, виставлення рахунків абонентам, обробку платежів. *Біллінгова система* - прикладне програмне забезпечення підтримки бізнес-процесів білінгу), перетворення адрес.

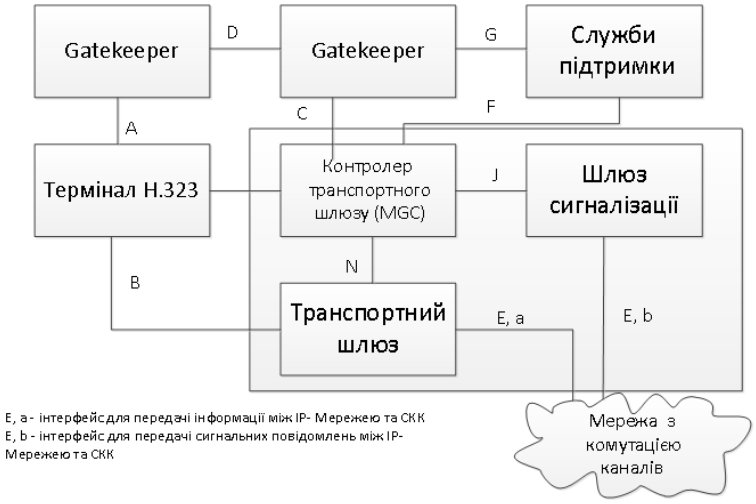

Рис.20. Функціональна архітектура, яка запропонована в межах проекту TIPHON

3. СИГНАЛІЗАЦІЯ В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

3.1 Загальні принципи сигналізації в мережах IP-телефонії

При впровадженні IP-телефонії важливим фактором є забезпечення сумісності систем різних виробників. Досягнення сумісності можливе тільки на базі стандартних протоколів сигналізації.

Протоколи сигналізації забезпечують встановлення, адміністрування та завершення сеансу зв’язку між кінцевими точками (користувачами), які ідентифікуються однозначно заданою схемою адресації. Поняття «сигналізація» відноситься до всієї інформації, яка пов’язана з викликами та необхідна для їх встановлення, маршрутизації, моніторингу і завершення як на фізичному, так і на логічному рівні.

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

У всіх сучасних мережах з комутацією каналів система сигналізації основана

на сімействі ЗКС №7. Вони забезпечують обмін повідомленнями, які необхідні для маршрутизації викликів, резервування ресурсів, трансляції адрес, встановлення з'єднань, управління ними, встановлення рахунків.

У порівнянні із сигналізацією у звичайних телефонних мережах сигналізація IP-телефонії повинна мати більш широкі можливості в силу специфіки кінцевих вузлів. Вони можуть мати найрізноманітніші характеристики в частині необхідної смуги пропускання, кодування/декодування аудіосигналів, передавання даних і т.д., і для встановлення сеансу зв`язку між ними необхідно впевнитися у сумісності цих характеристик.

В системах IP-телефонії процедури управління викликами виконуються протоколами сигналізації, а безпосередня маршрутизація трафіку через IP-мережу забезпечується протоколами: OSPF або BGP (резервування мережних ресурсів можливе, наприклад, за допомогою протоколу RSVP). Таким чином, архітектура мережі IP-телефонії передбачає розділення площин управління і передавання інформації користувачів, що є найбільш сприятливою умовою для впровадження нових послуг (рис.21).

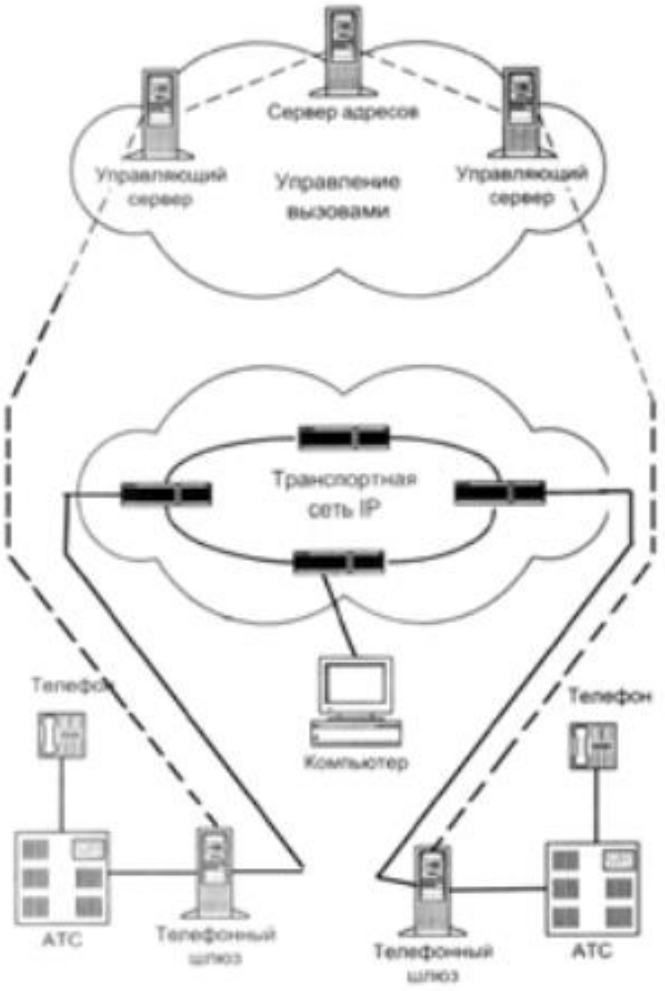

Рис.21. Управління викликами в мережі IP-телефонії

Ще одне важливе питання, яке пов'язане з сигналізацією в IP-телефонії –

контроль за доступом до мережі. У звичайній ТМЗК абонент підключається до АТС через фіксований місцевий шлейф, тому ідентифікувати його телефонний апарат дуже просто. В мережі IP-телефонії все більш складно, оскільки існує безліч різних способів доступу до неї: із звичайного телефону через ТМЗК, по модемному з'єднанню через сервер віддаленого доступу, через ЛОМ і територіально розподілену мережу і т.д. Крім того, користувачі можуть переміщатися між різними мережами, таким чином, абонента неможна ідентифікувати по лінії доступу, яка ним використовується.

Для ефективного контролю доступу оператор повинен аутентифікувати кожного користувача, який запитує послугу. Із збільшенням кількості операторів IP-телефонії потрібні також засоби контролю за трафіком на границі між їх мережами. Такі засоби повинні здійснювати контроль за доступом та використанням мережних ресурсів та виконанням угод по якості обслуговування. При їх відсутності оператору буде проблемно гарантувати користувачу визначений клас обслуговування, якщо його трафік – частково проходить через мережу іншого оператора.

На рис.22 показано місце механізмів сигналізації IP-телефонії у протокольному стеку: над ними знаходяться додатки, під ними – транспортні служби IP. Додаток може представляти собою телефонний шлюз.

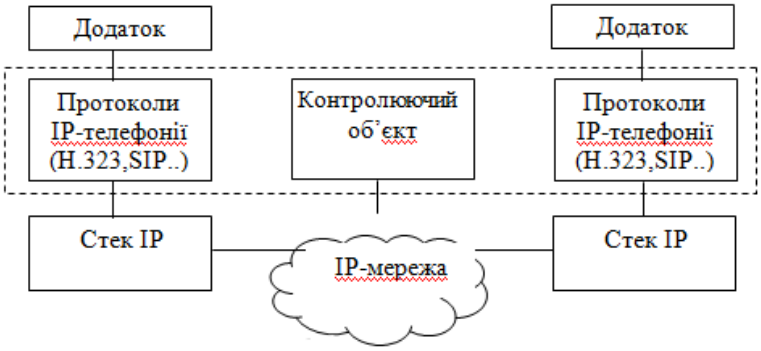

Рис.22. Механізми сигналізації IP-телефонії у протокольному стеку

У загальному випадку для встановлення з'єднання між викликаємим і викликаючим абонентом шлюзи IP-телефонії повинні:

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

Для виконання цих операцій на сьогодні використовуються різні протоколи сигналізації.

3.2 Сигналізація по стандарту H.323

У рекомендаціях H.323 описані об’єкти, які необхідні для мультимедійного зв’язку (передавання аудіо, відео та даних по мережам з комутацією пакетів, наприклад, по мережам IP), їх функції та способи взаємодії, зокрема алгоритми формування пакетів, стиснення аудіо- та відеоінформації. Крім того, рекомендація H.323 спрямована на вирішення задач адміністрування кінцевих користувачів, адресації, контролю за використанням смуги пропускання мережі та мережних об’єктів.

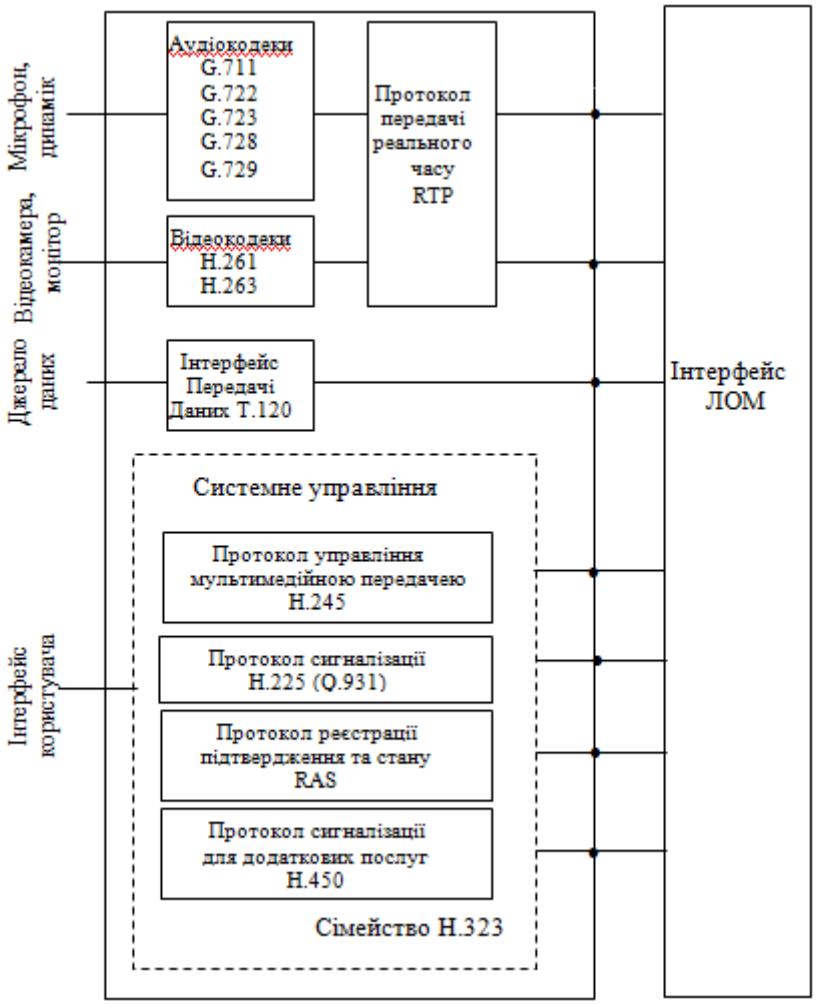

Рис.23. Сукупність рекомендацій H.323

Для виконання дій сигналізації між шлюзами та gatekeeper у відповідності з Рекомендацією MCE-T H.323 повинні використовуватися наступні протоколи:

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

Протокол сигналізації RAS (реєстрації, підтвердження та стану) використовується для передавання службових повідомлень між терміналами та

контролером зони H.323. RAS-повідомлення використовуються для реєстрації терміналів, допуску їх до сеансу зв'язку, зміни смуги пропускання, що використовується, інформування про стан сеансу та його завершення. При відсутності контролера зони (gatekeeper) протокол RAS не задіюється.

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

За допомогою сигналізації RAS здійснюється:

- знаходження gatekeeper, на якому можлива реєстрація кінцевого обладнання;
- реєстрація кінцевого пристрою;
- визначення географічного положення кінцевого пристрою;
- вказування необхідної смуги пропускання;
- зміна смуги пропускання.

Передавання повідомлень RAS здійснюється у дейтаграмах UDP. Для адресації RAS повинна використовуватися адресна інформація, в яку входять:

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

Мережна адреса є адресою у форматі, який використовується у мережі з комутацією пакетів, наприклад, адреса у форматі IPv4, IPv6.

Ідентифікатор TSAP використовується для ідентифікації інформаційних потоків, що відправлені з однієї мережної адреси. Для gatekeeper виділені постійні значення ідентифікатора TSAP: 1718 (для пошуку gatekeeper) та 1719 (для передавання повідомлень сигналізації RAS).

Мнемонічна адреса служить для адресації кінцевого обладнання у формі, яка зручна користувачу. Адресою може бути телефонний номер у форматі E.164, телефонний номер у корпоративній мережі, адреса електронної пошти. Gatekeeper не має мнемонічної адреси.

Знаходження gatekeeper повинно здійснюватися за допомогою широкомовного запиту GRQ (Gatekeeper Request), що передається кінцевим обладнанням з ідентифікатором TSAP, що дорівнює 1718. Якщо gatekeeper знайдений, і він готовий обслужити запит від кінцевого обладнання, у відповідь воно повинне отримати повідомлення GCF (Gatekeeper Confirm). Якщо кінцеве обладнання отримало відповідь від декількох gatekeeper, вибір одного з них повинен здійснюватися кінцевим обладнання довільним чином. Якщо gatekeeper не може обслужити запит від кінцевого обладнання, то у відповідь він повинен передати повідомлення GRJ (Gatekeeper Reject), в якому повинна повідомлятися причина відмови, і може міститися адреса альтернативного gatekeeper. При знаходженні

gatekeeper між ним та кінцевим обладнанням здійснюється встановлення логічного каналу сигналізації, по якому будуть передаватися інші повідомлення RAS (рис.24).

Рис.24. Етапи проходження виклику в середовищі H.323

Після знаходження gatekeeper кінцеве обладнання у повідомленні RRQ (Registration Request) повинно повідомити gatekeeper свою мережну та мнемонічну адресу. У відповідь gatekeeper повинен передати повідомлення RCF

(Registration Confirm) для підтвердження реєстрації кінцевого обладнання, або RRJ (Registration Reject) у випадку відмови від реєстрації. Повідомлення RRQ може передаватися при включенні кінцевого обладнання. Якщо при повторній реєстрації мнемонічна та мережна адреса, передані gatekeeper кінцевим обладнанням, співпадають з раніше переданими, то gatekeeper повинен передати повідомлення RCF. Якщо при повторній реєстрації мнемонічна адреса дорівнює раніше вказаній, а мережні відрізняються, повинне бути передане повідомлення RRJ з причиною відмови «duplicate registration». Для відміни реєстрації використовуються повідомлення URQ (Unregistered Request), що передається кінцевим обладнанням, і UCF (Unregistered confirm), URJ (Unregistered reject), що передаються gatekeeper кінцевому обладнанню.

Реєстрація кінцевого обладнання на gatekeeper може здійснюватися один раз і не повторюватися при включенні кінцевого обладнання. В цьому випадку gatekeeper повинен визначати стан кінцевого обладнання. Для цього gatekeeper повинен періодично передавати повідомлення IRQ (Information Request). Інтервал визначається виробником обладнання і повинен бути не менше 10 секунд.

Після реєстрації кінцевого обладнання на gatekeeper воно може встановити з'єднання з викликаємим кінцевим обладнанням. Для цього кінцеве обладнання-ініціатор повинне передати повідомлення ARQ (Admissions request) та встановити логічний канал для передавання повідомлень Q.931. У повідомленні ARQ вказуються швидкість передавання, яка кратна 100 біт/с, і кількість каналів, які необхідні для передавання мовної інформації. Наприклад, при використанні інтерфейсів ISDN для виділення смуги 192 кбіт/с необхідно вказати значення відповідно 640 та 3. Швидкість вказується без урахування розмірів заголовків пакетів та блоків даних транспортних протоколів. Якщо ж мережа може забезпечити потрібні параметри, то gatekeeper повинен передати підтвердження ACF (Admissions Confirm), у противному випадку передається повідомлення ARJ (Admissions Reject) із вказуванням причини відмови.

Після отримання підтвердження кінцеве обладнання встановлює з'єднання з викликаємим кінцевим обладнанням з використанням ***сигналізації Q.931 (згідно H.225.0).*** Повідомлення сигналізації Q.931 можуть передаватися по логічному каналу через gatekeeper або безпосередньо між двома кінцевими пристроями. Вибір способу здійснює gatekeeper та повідомляє про це кінцевому обладнанню у повідомленні ACF.

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

Для встановлення з'єднання використовуються повідомлення ***Setup*** і ***Connect,***

після передавання яких встановлюється канал управління H.245. Канал для передавання інформації управління H.245 може бути встановлений двома способами: через gatekeeper або безпосередньо між кінцевими пристроями. У випадку, якщо логічний канал сигналізації Q.931 встановлюється через gatekeeper, то канал для передавання інформації управління H.245 також повинен встановлюватися через gatekeeper.

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

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

Стандарт H.225 описує протоколи сигналізації та формування пакетів у системах пакетного передавання мультимедійного трафіку. *Канал управління викликами H.225.0* використовується для встановлення та розриву з'єднань між двома терміналами H.323, а також між терміналом та шлюзом. Службові повідомлення цього протоколу передаються поверх TCP або UDP (рис.25). Відповідний механізм H.225.0 оснований на протоколі Q.931. Він забезпечує надання цілого ряду додаткових видів обслуговування та можливість взаємодії з мережами, які базуються на комутації каналів. Канал управління викликами не залежить від каналу RAS та каналу управління H.245.

Рис.25. Додаток H.225.0 у стеку протоколів H.323

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

процедури підтвердження сигнальної інформації для забезпечення гарантії надійного передавання аудіовізуальної інформації та даних.

Рекомендація охоплює широкий діапазон додатків, включаючи зберігання/повторне передавання, передавання повідомлень та розподіл послуг, а також забезпечення діалогу.

Протокол управління мультимедійним передаванням Н.245 забезпечує:

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

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

За допомогою сигналізації Q.931 згідно рекомендації МСЕ-Т Н.225.0 та протоколу управління Н.245 повинно здійснюватися:

- передавання запиту на встановлення з’єднання;
- ініціалізація з’єднання та обмін інформацією про можливості;
- встановлення з’єднання для передавання голосової інформації;
- роз’єднання з’єднання.

Для встановлення з’єднання ініціатор виклику (кінцеве обладнання 1) повинне передати повідомлення Setup кінцевому обладнанню 2 по логічному каналу сигналізації з ідентифікатором TSAP, який дорівнює 1719.

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

Після отримання повідомлення Connect повинен бути встановлений логічний канал управління Н.245, по якому передається інформація про можливості кінцевого обладнання у повідомленні terminal Capability Set.

Для визначення ініціатора встановлення каналу RTP використовується ідентифікатор status Determination Number у повідомленні Master Slave Determination.

Після ініціалізації з’єднання створюється логічний канал для передавання голосової інформації. Встановлення каналу для передавання голосової інформації

здійснюється кінцевим обладнанням після отримання повідомлення open Logical Channel по каналу управління H.245. Передавання голосової інформації по логічному каналу повинне здійснюватися у пакетах RTP. Передавання управляючої інформації повинне здійснюватися у пакетах RTCP.

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

Зменшення смуги пропускання можливе завжди, а для збільшення смуги пропускання вище значення, яке вказане в останньому повідомленні ARQ, кінцеве обладнання повинне закрити всі логічні канали і відкрити їх заново. Логічний канал повинен бути закритий повідомленням close Logical Channel протоколу управління H.245, а відкритий з новими параметрами повідомленням open Logical Channel.

З'єднання роз'єднується наступним чином:

- ініціатор роз'єднання повинен закрити канал повідомленням close Logical Channel, що передається по каналу управління H.245;
- ініціатор роз'єднання повинен передати повідомлення end Session Command, що передається по каналу управління H.245;
- віддалене обладнання очікує повідомлення end Session Command, що передається по каналу управління H.245;
- якщо логічний канал сигналізації Q.931 відкритий. Він закривається повідомленням Release Complete.

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

3.3 Сигналізація на основі протоколу SIP

Протокол SIP (Session Initiation Protocol) є протоколом прикладного рівня, який розроблений робочою групою по управлінню багатоточковими сеансами мультимедіазв`язку (MMUSIC) організації IETE (Рекомендація RFC 2543). Він дозволяє організувати і провести такий сеанс, забезпечуючи його встановлення, модифікацію і завершення. SIP – протокол прикладного рівня, який працює поверх TCP або UDP. SIP займається тільки встановленням, управлінням та розривом з'єднань.

В основу протоколу SIP закладені наступні принципи:

- Персональна мобільність користувачів. Користувачі можуть переміщатися без обмежень в межах мережі.
- Масштабуємість мережі.
- Розширюваність протоколу. Можливість доповнення протоколу новими функціями при введенні нових послуг та його адаптація до роботи з різними додатками.
- Інтеграція в стек існуючих протоколів Інтернету, розроблених IETF.
- Взаємодія з іншими протоколами сигналізації. Протокол SIP може бути використаний разом з протоколом H.323.

Функції, які підтримуються протоколом SIP:

- Положення користувача (user location). Протокол SIP дозволяє виявити положення кінцевого користувача, щоб встановити сеанс зв'язку або передати запит SIP. Мобільність користувача (user mobility) від самого початку підтримується протоколом SIP.
- Можливості користувача (user capabilities). Протокол SIP дозволяє з'ясовувати можливості середовища передавання і пристроїв, які приймають участь у сеансі.
- Доступність користувача (user availability). Протокол SIP дозволяє з'ясувати готовність кінцевого користувача встановити зв'язок.
- Встановлення сеансів (session setup). Протокол SIP дозволяє встановити параметри сеансу для сторін, які приймають участь у ньому.
- Обробка сеансу (session handling). Протокол SIP дозволяє модифікувати, передавати та завершувати активний сеанс.

Мережні елементи протоколу SIP

Мережа SIP зазвичай містить наступні пристрої:

- *Агент користувача (User Agent - UA);*
- *Клієнтський агент користувача (User Agent Client - UAC);*
- *Серверний агент користувача (User Agent Server - UAS);*
- *Проксі-сервер (Proxy);*
- *Сервер переадресації (redirect server)* – це агент UAS, який створює відповіді SIP класу 300 на отримані запити, переадресовуючи агент UAC по альтернативному набору *універсальних ідентифікаторів ресурсу (Uniform Resource Identifier - URI);*
- *Сервер реєстрації (registrar server).* Агент UAS, який приймає запити SIP REGISTER та переносить інформацію із запиту в базу даних розташувань;
- *Взаємний агент користувача (Back-To-Back User Agent – B2BUA).* Проміжний об'єкт, який обробляє вхідні запити SIP як агент UAS. Щоб відповідати на вхідні запити SIP, агент B2BUA діє як агент UAC, відновлюючи

запит SIP і надсилаючи його по мережі. Агент B2BUA повинен підтримувати стан діалогу та приймати участь у всіх транзакціях діалогу.

SIP працює по схемі *клієнт-сервер* (рис.26): клієнт виконує запит визначеного типу сервісу, а сервер обробляє його запит і забезпечує надавання сервісу. Згідно протоколу SIP, система користувачів може не тільки формувати, але й приймати запити. Це означає, що вона повинна бути обладнана й клієнтською (клієнт агента користувача – UAC) і серверною (сервер агента користувача – UAS) частинами.

Клієнтський агент користувача (User Agent Client - UAC) – логічна функція, яка ініціює запити SIP та приймає відповіді SIP. Прикладами роботи агента UAC є ініціалізація телефонного запиту SIP від імені користувача або перенаправлення запиту проксі-серверу від імені UAC.

Серверний агент користувача (User Agent Server - UAS) – логічна функція, яка приймає запити SIP і відправляє назад відповіді SIP. Телефон SIP, наприклад, приймає такі запити, як INVITE.

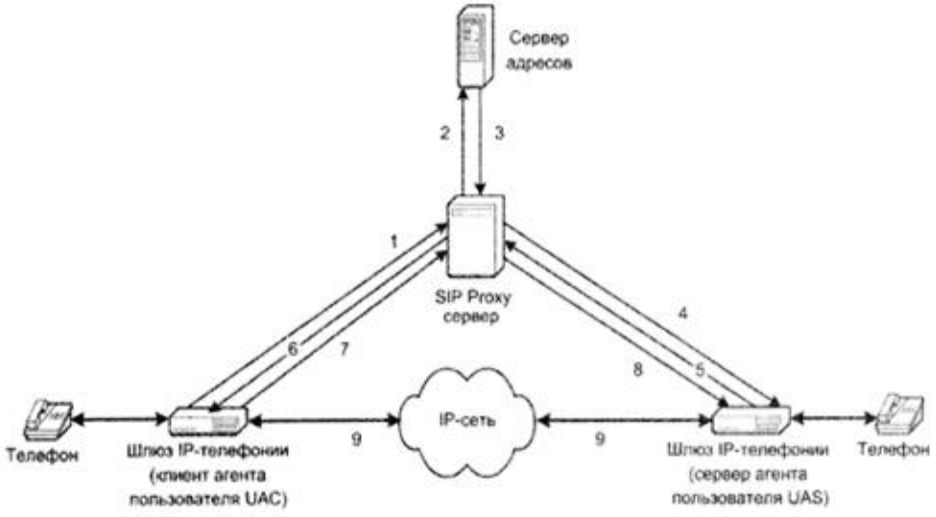

Рис.26. Схема сигналізації по протоколу SIP

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

У протоколі SIP визначені два види сигнальних повідомлень - *запит* і *відповідь*. Вони мають текстовий формат (кодування символів згідно RFC 2279) і базуються на протоколі HTTP (синтаксис і семантика визначені у RFC 2068). У *запиті* вказуються процедури, що викликаються для виконання необхідних операцій, а у *відповіді* - результати їх виконання.

Запити SIP (SIP request) – це повідомлення, які передаються від клієнта серверу, щоб він здійснив операцію SIP.

У документі RFC 3261 визначено шість наступних запитів SIP або методів, які

дозволяють агенту UA та проксі-серверу знаходити ти користувачів, а також ініціювати, модифікувати та завершати сеанси (визначено шість процедур):

- **INVITE** - запрошує користувача взяти участь у сеансі зв'язку (служить для встановлення нового з'єднання; може містити параметри для узгодження). Повідомлення INVITE можна також використовувати для зміни характеристик сеансу, який раніше встановлений. Позитивна відповідь на запит INVITE (відповідь 200 OK) означає готовність викликаємої сторони приймати участь у створюваному мультимедійному сеансі;

- **BYE** - завершує з'єднання між двома користувачами;

-**OPTIONS** - використовується для передавання інформації про характеристики, які підтримуються (це передавання може здійснюватися напряму між двома агентами користувачів або через сервер SIP);

- **ACK** - використовується для підтвердження отримання повідомлення або для позитивної відповіді на команду INVITE. Повідомлення ACK використовується тільки з запитами INVITE. Повідомлення ACK передається безпосередньо після відповіді 200 OK. Проксі-сервери транзитних ділянок та агенти UAC надсилають повідомлення ACK у відповідь на інші фінальні відповіді;

- **CANCEL** - припиняє пошук користувача;

- **REGISTER** - передає інформацію про місцезнаходження користувача на сервер SIP, який може транслювати її на сервер адрес (Location Server).

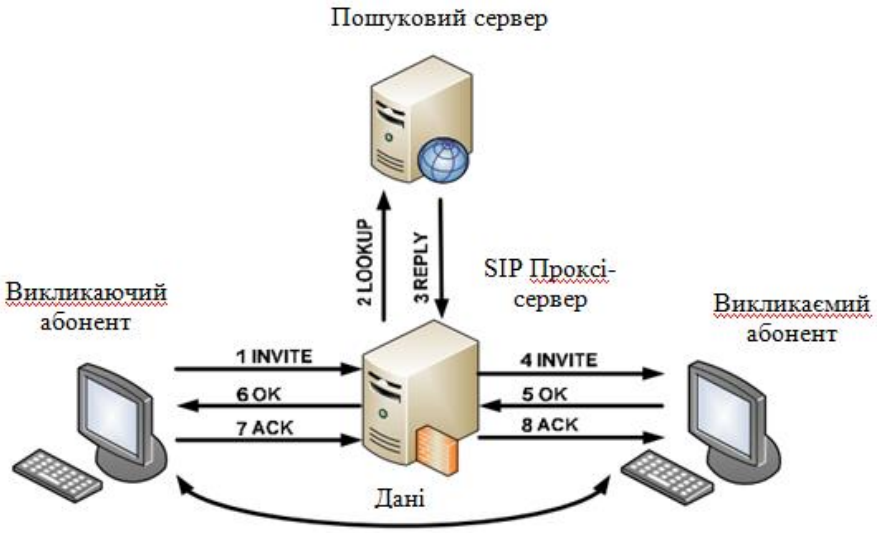

Рис.27. Архітектура мережі SIP

SIP використовує механізм SDP (Session Description Protocol) для опису характеристик сеансу: часу проведення, необхідні ресурси і т.д. (Рекомендації RFC 2327). SDP використовується виключно для текстового опису сеансу і не має ні транспортних механізмів, ні засобів узгодження необхідних для сеансу параметрів. Ці функції повинні виконувати протоколи, які застосовуються для передавання інформації SDP.

Сервер надсилає клієнту відповідь SIP для того, щоб сповістити його про стан запиту SIP, який надісланий клієнтом на сервер раніше. Агенти UAS та проксі-сервери створюють відповіді SIP на запити SIP для того, щоб ініціалізувати агент UAC. Відповіді SIP пронумеровані від 100 до 699 та згруповані як 1xx, 2xx і т.д. до 6xx. За класифікацією вони розділені на *попередні* (provisional) та *кінцеві* (final) або фінальні.

Попередня відповідь означає, що сервер працює, але це некінцевий результат обробки запиту SIP. Відповіді SIP класу 1xx відносяться до попереднього стану. Завершення обробки та фінальний стан запиту SIP означає кінцеву відповідь. Усі відповіді класів 2xx, 3xx, 4xx, 5xx та 6xx є кінцевими.

- Відповідь класу 2xx означає успішну обробку запиту SIP.
- Відповідь класу 3xx означає, що запит SIP повинен бути переадресований для обробки на інший агент UAS;
- Відповідь класу 4xx, 5xx або 6xx означає відмову в обробці запиту SIP.

Повідомлення-відповіді можуть містити шість типів можливих результатів:
- запит у процесі виконання (1xx);
- успішний запит (2xx);
- переадресація (3xx);
- невірний запит (4xx);
- відмова сервера (5xx);
- глобальна відмова (6xx).

Адресація, яка використовується в SIP, основана на уніфікованому вказівнику ресурсів SIP URL, в якому може бути записане ім`я домену (user@domain) або IP-адреса (user@IPadress) користувача. Мета використання даного формату – інтеграція SIP-послуг із існуючими службами Інтернет. Сервер імен доменів (DNS) перетворює доменні імена у IP-адреси кінцевої точки (рис.8). Вся маршрутизація та передавання мультимедійних потоків виконується IP-мережею знизу. Таким чином, послуги SIP добре інтегруються у традиційну модель Web-комунікацій із сервером DNS, який забезпечує перетворення доменного імені у мережну адресу.

Призначений для ініціації сеансів протокол SIP забезпечує визначення адреси користувача і встановлення з'єднання з ним. Крім цього, він є основою для використання інших протоколів, що реалізують функції захисту, аутентифікації, опису каналу мультимедійного зв'язку і т.д. Для білінгу, наприклад, може використовуватися протокол Radius.

Прикладом реалізації протоколу SIP может служити програмна платформа eConvergence Server Solutions фірми Dynamicsoft, яка включає наступні продукти:

- ***SIP Proxy Server*** - маршрутизатор між кінцевими точками, кожна з яких визначена як UAC або UAS; на додаток до функцій забезпечення взаємодії

між різними серверами платформи він надає послуги перенаправлення і реєстрації/визначення місця розташування користувачів.

Проксі-сервер – це проміжний об’єкт у мережі SIP, який відповідає за пере направлення запитів SIP цільовому агенту UAS або іншому проксі-серверу від імені агента UAC. Але, в першу чергу, проксі сервер здійснює маршрутизацію в мережі SIP;

- ***SIP Location Server*** - забезпечує безпечну сигналізацію викликів, зберігає інформацію про користувачів, яка необхідна сервіс-провайдерам для гнучкого управління доступом користувачів і маршрутизації викликів з метою надання найкращої якості послуги;
- ***SIP User Agent*** - управляє з'єднаннями між вихідною і вхідною сторонами, забезпечуючи підтримку необхідної якості послуг. Агент UA здатний виступати в ролі клієнта або сервера транзакцій SIP. Агент UA володіє *фіксацією стану* (stateful), тобто він здатний зберігати стан сеансу або діалогу;
- ***SIP CallAccounting Server*** - виконує функції збору і обробки інформації у вигляді детальних звітів про транзакції TDR, які отримані від SIP Proxy Server, яка в подальшому може бути використана в системах білінгу і менеджменту користувачів.

Протокол SIP є одноранговим, тобто його мережні можливості, такі як маршрутизація виклику та функції управління сеансами, розподілені між всіма вузлами (включаючи кінцеві точки та мережні сервери) мережі SIP. Це суттєво відрізняється від традиційної моделі телефонної мережі, де телефони (або пристрої кінцевого користувача) повністю залежать від центрального комутатора – як при встановленні виклику, так і при надаванні інших послуг.

Взаємодія з іншими протоколами IETF

Сам по собі агент SIP не забезпечує всіх тих можливостей, які необхідні для встановлення інтерактивного мультимедійного сеансу. Замість цього протокол SIP, який є частиною середовища виконання стандартних протоколів, створює мультимедійну архітектуру.

Агенти SIP та додатки потребують й інших протоколів:

- *Для опису характеристик сеансу.* Чи є сеанс звуковим або відео сеансом, які кодеки він використовує, що представляє собою мультимедійне джерело і яка адреса отримувача.

- *Для обробки мультимедійних даних.* Протоколи, які контролюють і передають звукові та відео пакети сеансу.

- *Для підтримки функцій* аутентифікації, авторизації та обліку; резервування мережних ресурсів; вибору шлюзу та розподілу навантаження; перетворення IP-адрес в імена хостів; запобігання підслуховування, втручання або підробки повідомлень.

Сеанси, які встановлені з використанням протоколу SIP, зазвичай використовують наступні протоколи IETF.

- Система DNS. Встановлення сеансу SIP може вимагати використання системи доменних імен DNS (Domain Name System) для пошуку хоста або імені домену серед маршрутизуємих IP-адрес. Систему DNS можна також використовувати для розподілу навантаження по декільком серверам у кластері, що ідентифікується по імені хоста.
- Протокол опису сеансу зв'язку (Session Description Protocol - SDP). Запис SDP у тілі повідомлення SIP використовується для опису параметрів мультимедійного сеансу. Ця інформація включає тип сеансу, наприклад, звук, відео або і те, і інше, а також деякі параметри, наприклад, кодеки та порти, які необхідні для встановлення мультимедійного потоку. Протокол SDP визначений у документі RFC 2327.
- Протокол RTP. Визначений у документі RFC 1889 і відповідає за транспортування даних (звукових або відео пакетів) у реальному масштабі часу до кінцевих точок, що приймають участь у сеансі. Протокол управління у реальному масштабі часу RTCP (Real Time Control Protocol), визначений у документі RFC 1890, забезпечує якість обслуговування (QoS) при зворотному зв'язку з відправником. Документ RFC 3550 випущений для заміни документа RFC 1889.
- Протокол RSVP. Протокол SIP може використовувати протокол RSVP для резервування мережних ресурсів, таких як смуга пропускання, ще до встановлення мультимедійного сеансу. Це гарантує, що мережні ресурси викликаємої сторони будуть вже приведені до готовності, коли надійде вхідний виклик.
- Протокол TLS (Transport Layer Security) – протокол забезпечення безпеки на транспортному рівні. Протокол SIP рекомендує використання протоколу TLS, який визначений у документі RFC 2246, для забезпечення секретності та цілісності сигнальної інформації SIP під час передавання по мережі. Протокол TLS дозволяє клієнтським та серверним додаткам впізнавати один одного, проводити перемови, застосовувати алгоритми шифрування та встановлювати криптографічні ключі перед передаванням сигнальної інформації по мережі.

Проста мережа SIP містить:

- проксі-сервери SIP;
- агенти користувача, які з'єднані з комутованою PSTN.

Агент UAC протоколу SIP, проксі-сервери та шлюз SIP/PSTN розміщені всередині мережі IP. Шлюз SIP/PSTN володіє магістралями SS7/PRI, що підключені до комутатора PSTN.

Суцільними лініями між обладнанням позначають запити SIP, а штрих пунктирними – відповіді SIP.

Адресація SIP

Адреси SIP ідентифікують користувача або ресурс всередині мережного домену. Адреси SIP звичайно називають *SIP URI*. Як правило, адреса SIP URI – це звичайна адреса електронної пошти в одному із наступних форматів:

sip: користувач@домен:порт

або

sip: користувач@хост:порт

Поле *користувач* ідентифікує користувача за іменем, наприклад, *john.doe* (Джон До), або по номеру телефона, наприклад, 40812345, у контексті домену або хоста. Поле *порт* необов'язкове. Якщо номер порта не вказаний явно, для повідомлень SIP URI за замовчуванням заданий порт 5060. Але, якщо номер порта буде вказаний, то використовувати потрібно буде саме його. Нижче приведені приклади адрес SIP URI:

sip: join.doe@company.com

sip: 40812345@proxy1.company.com

Для організації взаємодії з існуючими додатками IP-мереж і для забезпечення мобільності користувачів протокол SIP використовує адресу, подібно адресі електронної пошти.

SIP-адреси бувають чотирьох видів:

- ім'я@домен;
- ім'я@хост;
- ім'я@IP-адреса;
- №телефону@шлюз.

Перша частина – це ім'я користувача, зареєстрованого у домені або на робочій станції.

Друга частина – ім'я домену, робочої станції або шлюзу.

- *sip:als@rts.loniis.ua*
- *sip:user1@192.168.100.152*
- sip:294-75-47@gateway.ua

Протоколи транспортного рівня для передавання сигналів SIP

Транзакції SIP використовують як протоколи транспортного рівня, які вимагають встановлення з'єднання (наприклад, протокол TCP або *протокол управління передаванням потоку* (Stream Control Transmission Protocol – SCTP)),

так і протоколи, які не вимагають встановлення з'єднання (наприклад, протокол UDP). Для протоколів, які не вимагають встановлення з'єднання, протокол SIP визначає, що додаток SIP запускає таймер повторного передавання, щоб, повторюючи запити SIP, гарантувати наскрізну надійність.

3.4 Порівняння протоколів H.323 та SIP

SIP базується на архітектурі клієнт-сервер, що дозволяє забезпечувати управління викликами на рівні сервера. Служби SIP орієнтовані на інтеграцію із службами Інтернет.

Технологія H.323 надає більше можливостей по управлінню визначеною послугою у частині аутентифікації та обліку і контролю за використанням мережних ресурсів. Можливості протоколу SIP тут значно менші. Вибір цього протоколу компанією постачальником послуг фактично означає, що технологічна інтеграція послуг для неї важливіше можливостей гнучкої тарифікації та контролю за використанням мережних ресурсів.

В цілому можна зробити висновок, що протокол SIP орієнтований на Інтернет - провайдерів, які розглядають послуги Інтернет-телефонії лише як невелику частину свого сервісного пакету. Будучи самодостатньою, технології H.323 більше підходить для корпоративних мереж (інтранет) і постачальників послуг IP-телефонії, для яких ці послуги не є домінуючими. В цілому H.323 і SIP не потрібно розглядати як конкурентні технології, вони є різними підходами, що призначені для різних сегментів ринку. Вони можуть працювати паралельно і навіть взаємодіяти через спеціальний пограничний шлюз.

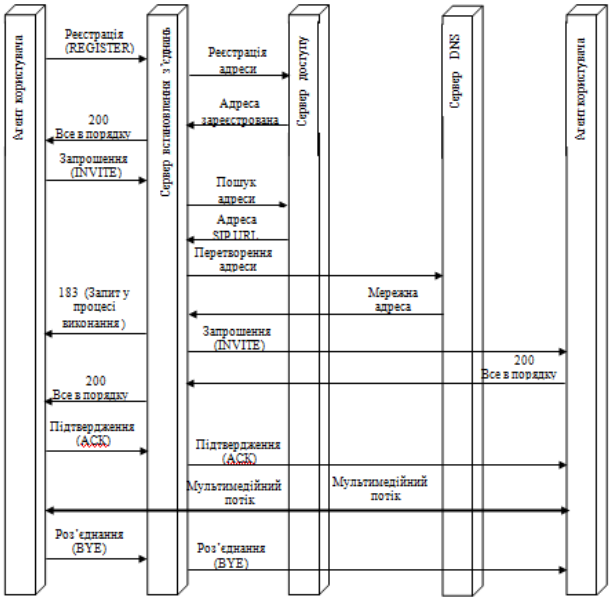

Рис.28. Можливий сценарій встановлення і завершення сеансу зв'язку по протоколу SIP

3.5 Особливості сигналізації за концепцією TIPHON

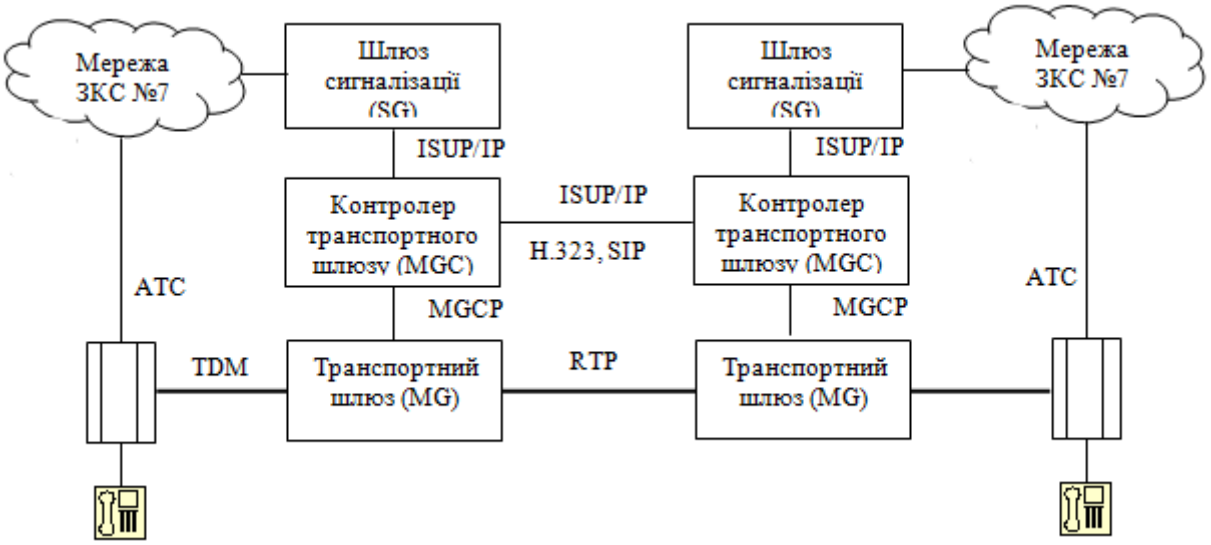

Рис.29. Функціональна модель мережі по проекту TIPHON

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

MGC аналізує інформацію сигналізації та передає управляючу інформацію у транспортний шлюз за допомогою спеціального протоколу управління, в задачі якого входить забезпечення управління різними ресурсами (системою інтерактивного голосового відгуку, мостами конференцзв'язку і т.д.), прийомом та формуванням сигналів DTMF, формуванням тональних сигналів (готовності до набору номера, контроля посилки виклику, "зайнято" та ін.), ехо-подавленням, використанням кодеків (G.711, G.723.1, G.729, GSM і т.д.), збором статистики, тестуванням кінцевих точок (наприклад, випробовування шлейфу), резервуванням, роз'єднанням та блокуванням кінцевих точок, шифруванням.

Протокол управління транспортними шлюзами MGCP представляє собою досить простий протокол клієнт-сервер. Логіка управління викликами виконується агентом (Call Agent), що знаходиться поза транспортним шлюзом. Сам транспортний шлюз представляється у вигляді об'єкта, який складається із кінцевих точок – точок входу/виходу інформаційних потоків та з'єднань – двох або більше з'єднаних кінцевих точок. Модель визначає фізичні кінцеві точки

(наприклад, закінчення з'єднувальних ліній) та віртуальні кінцеві точки (наприклад, аудіоджерела). Сам протокол MGCP використовує принцип «провідний/ведений», згідно якого агент управління викликами передає транспортному шлюзу команди для управління кінцевими точками та з'єднаннями, а також ініціації визначених дій.

MGCP є досить універсальним протоколом, здатним забезпечити розподілене управління різними типами транспортних шлюзів, зокрема телефонними шлюзами і серверами доступу. Він може використовуватися для встановлення з'єднання та виконання різних функцій обслуговування, наприклад, тестування шлейфу.

Подальшим розвитком протоколу MGCP є протокол управління викликами Megaco (Media Gateway Control), відомий також як стандарт ITU H.248, який визначає взаємодію, з одного боку, шлюзу між різними засобами передавання даних (Media Gateway, MG) та з іншого – контролеру шлюзів між середовищами передавання даних (Media Gateway Controller, MGC) (рис.30). Іншими словами, Megaco розроблений для внутрішньо-доменного віддаленого управління пристроями, що відповідають за встановлення з'єднання або проведення сеансу зв'язку, включаючи шлюзи VoIP, сервери віддаленого доступу, мультимлексори цифрових абонентських ліній (Digital Subscriber Line Access Multiplexer, DSLAM), маршрутизатори з підтримкою багатопротокольної комутації з використанням міток (Multiprotocol Label Switching, MPLS), оптичні крос-конектори, модулі агрегування сеансів PPP та ін.

Рис.30. Використання протоколу Megaco в мережі IP-телефонії

MGCP та Megaco повідомляють шлюзу, яким чином зв'язати потоки, що надходять у мережу з комутацією пакетів або комірок, з потоками пакетів або комірок, що переносяться, наприклад, транспортним протоколом реального часу RTP. Megaco повторює MGCP відносно архітектури та взаємодії контролера із шлюзом, але при цьому Megaco підтримує більш широкий діапазон мережних технологій, в тому числі й ATM.

Типовим прикладом роботи протоколу MGCP є перевірка стану кінцевої точки

на предмет зняття трубки (яку знімає абонент, щоб виконати дзвінок). Після фіксації події «зняття трубки» шлюз повідомляє про це контролеру, після чого останній може надіслати шлюзу команду подати в лінію неперервний гудок і чекати тональних сигналів DTMF номеру абонента, який набирається. Після отримання номеру контролер вирішує, по якому маршруту потрібно направити виклик, і, використовуючи протокол сигналізації між контролерами, в тому числі H.323, SIP або Q.BICC, взаємодіє із кінцевим контролером. Кінцевий контролер надає відповідному шлюзу вказівку подати дзвінок на викликаємо лінію. Коли цей шлюз визначає, що викликає мий абонент зняв трубку, обидва контролери надають відповідним шлюзам команди на встановлення двостороннього голосового зв'язку по мережі передавання даних. Таким способом дані протоколи розпізнають стани кінцевих точок, повідомляють про ці стани контролер, генерують у лінії сигнали (наприклад, неперервний гудок), а також формують потоки даних між підключеними до шлюзу кінцевими точками та мережею передавання даних, наприклад потоки RTP.

4. ЗАБЕЗПЕЧЕННЯ ЯКОСТІ IP-ТЕЛЕФОНІЇ

4.1 Показники якості IP – телефонії

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

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

Транспортні протоколи стеку TCP/IP, які функціонують над протоколом IP, не забезпечують високої якості обслуговування трафіку, чутливого до затримок. Необхідно забезпечити механізми, по яким в періоди перевантаження пакети з інформацією, чутливою до затримок (наприклад, мова), не будуть простоювати в чергах або отримають більш високий пріоритет, ніж пакети з інформацією, не чутливою до затримок.

У мережі повинні бути реалізовані механізми, які гарантують необхідну якість обслуговування (Quality of Service - QoS).

Заходи забезпечення QoS, що застосовуються в IP- мережах:

- Резервування ресурсів (на час з'єднання запитуються і резервуються необхідні для виконання додатку ресурси).
- Пріоритезація трафіку (поділ трафіку в мережі на класи з пріоритетним порядком обслуговування деяких із них).
- Перемаршрутізація (дозволяє при перевантаженні в мережі перевести трафік на резервний маршрут).

У сучасних IP-мережах перераховані заходи реалізуються за допомогою технологій IntServ, DiffServ і MPLS з використанням протоколу RSVP.

Основними складовими якості IP - телефонії є (рис.31):

• Якість мови, яка включає:

- ***діалог*** - можливість користувача зв'язуватися і розмовляти з іншим користувачем в реальному часі та повнодуплексному режимі;
- ***розбірливість*** - чистота і тональність мови;
- ***відлуння*** - 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 та фіксація сигналів багаточастотного набору номера.

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

- Фактори якості IP – мережі:

- *максимальна пропускна спроможність* – максимальна кількість корисних та надлишкових даних, яку вона передає;
- *затримка* – проміжок часу, який необхідний для передавання пакету через мережу;
- *джиттер* – затримка між двома послідовними пакетами;
- *втрата пакету* – пакети або дані, які втрачені під час передавання через мережу.

- Фактори якості шлюзу:

- *необхідна смуга пропускання* - різні вокодери вимагають різну смугу. Наприклад, вокодер G.723 вимагає смугу 16,3 кбіт/с для кожного мовного каналу;
- *затримка* - час, необхідний цифровому сигнального процесору DSP або іншим пристроям обробки для кодування і декодування мовного сигналу;
- *буфер джиттера* - збереження пакетів даних до тих пір, поки всі пакети не будуть отримані і потім можна буде передати частину мовної інформації у потрібній послідовності для мінімізації джиттера;

- *втрата пакетів* - втрата пакетів при стисканні і/або передаванні в обладнанні IP - телефонії;
- *подавлення відлуння* - механізм для подавлення відлуння, що виникає при передаванні по мережі;
- *управління рівнем* - можливість регулювати гучність мови.

Рис.31. Фактори, які впливають на якість IP-телефонії

4.2 Вплив мережі на показники якості IP-телефонії

Затримка

Затримка створює незручність при веденні діалогу, призводить до перекриття розмов і виникнення відлуння. Відлуння виникає у випадку, коли відбитий мовний сигнал разом з сигналом від видаленого кінця повертається знову у вухо того, хто говорить. Відлуння стає важкою проблемою, коли затримка в петлі передавання більше, ніж 50 мс. Так як відлуння є проблемою якості, системи з пакетною комутацією мови повинні мати можливість управляти відлунням і використовувати ефективні методи ехоподавлення.

Затруднення діалогу і перекриття розмов стають серйозним питанням якості, коли затримка в одному напрямку передавання перевищує 250 мс. Можна виділити наступні джерела затримки при пакетному передаванні мови з кінця в кінець (рис.32):

• *Затримка накопичення* (іноді називається алгоритмічної затримкою): ця затримка обумовлена необхідністю збору кадру мовних відліків, яка виконується у мовному кодері. Величина затримки визначається типом мовного кодеру і змінюється від невеликих величин (0,125 мкс) до декількох мілісекунд. Наприклад, стандартні мовні кодери мають наступні тривалості 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 у пакети для передавання через пакетну мережу створює визначені затримки. Затримка кодування або обробки залежить від швидкості роботи процесору і від типу алгоритму обробки, який використовується. Для зменшення завантаження пакетної мережі звичайно декілька кадрів мовного кодеру об'єднуються в один пакет. Наприклад, три кадри кодових слів G.729, які відповідають 30 мс мови, можуть бути об'єднані для зменшення розміру одного пакету.

• *Мережна затримка:* затримка, яка обумовлена фізичним середовищем та протоколами, які використовують для передавання мовних даних, а також буферами, що використовуються для видалення джиттера пакетів на прийомному боці. Мережна затримка залежить від ємності мережі та процесів передавання пакетів у мережі.

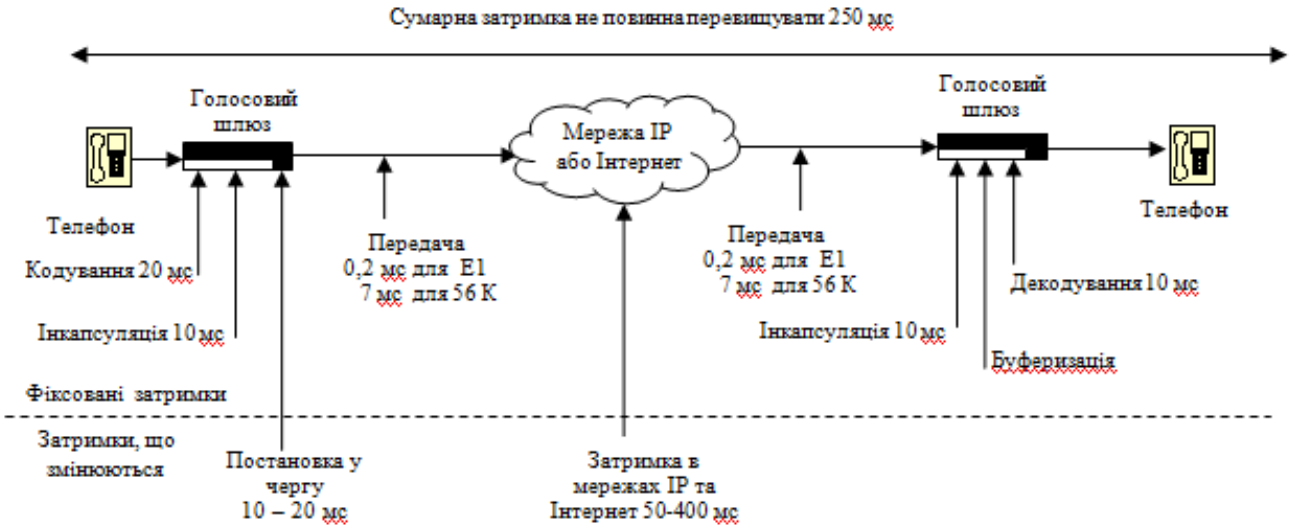

Рис.32. Складові затримки у мережі IP-телефонії

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

- *перший рівень* до 200 мс – відмінна якість зв’язку. Для порівняння, в PSTN допустимі затримки до 150-200 мс;
- *другий рівень* до 400 мс – вважається гарною якістю зв’язку. Але, якщо порівнювати з якістю зв’язку по мережам PSTN, то різниця буде очевидною. Якщо затримки постійно утримуються на верхній межі 2-го рівня (на 400 мс), то не рекомендується використовувати цей зв’язок для ділових перемов;

- *третій рівень* до 700 мс – вважається прийнятною якістю зв'язку для ведення неділових перемов. Така якість зв'язку можлива також при передаванні пакетів по супутниковому зв'язку.

Якість Інтернет-телефонії попадає під 2-3 рівні, причому неможливо впевнено сказати, що той чи інший провайдер Інтернет-телефонії працює по другому рівню, так як затримки в мережі Інтернет змінюються. Більш точно можна сказати про провайдерів IP-телефонії, які працюють по виділеним каналам. Вони попадають 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.

Джиттер

Коли мова або дані розбиваються на пакети для передавання через IP-мережу, пакети часто прибувають у пункт призначення у різний час і з різною послідовністю. Це створює розкид часу доставки пакетів (джиттер). Джиттер призводить до специфічних порушень передавання мови, які чуються як тріскіт та клацання. Розрізняють три форми джиттера:

1) *Джитер, який залежить від даних* (Data Dependent Jitter - DDJ) – виникає у випадку обмеженої смуги пропускання або при порушеннях у мережних компонентах;

2) *Спотворення робочого циклу* (Duty Cycle Distortion - DCD) – обумовлене затримкою розповсюдження між передаванням знизу вгору і зверху вниз;

3) *Випадковий джиттер* (Random Jitter - RJ) – є результатом теплового шуму.

Причини появи джиттера:

- ***Вплив мережі***. Нестійкий і погано передбачуваний час проходження пакету через мережу.
- ***Вплив операційної системи.*** Затримка у просуванні даних між мережним інтерфейсом і зовнішнім пристроєм голосового виведення становить, незалежно від алгоритму кодування мови, який використовується, величину в декілька десятків мілісекунд або навіть більше.
- ***Вплив джиттер-буфера.*** Занадто короткий буфер буде призводити до частих втрат пакетів, які запізнилися, а занадто довгий – до неприйнятно великої додаткової затримки. Зазвичай передбачається динамічне підстроювання довжини буферу.
- ***Вплив кодеку і кількості переданих у пакеті кадрів.*** Протягом часу, що визначається довжиною кадру кодека, повинна накопичуватися певної довжини послідовність цифрових представлень відліків. Крім того, деяким кодекам необхідний попередній аналіз більшої кількості голосової інформації, ніж повинно міститися в кадрі.

Джиттер - випадкова затримка розповсюдження пакету. Обумовлюється джиттер трьома факторами: обмежена смуга пропускання або некоректна робота активних мережних пристроїв; висока затримка розповсюдження сигналу; тепловий шум.

Найбільш часто застосовується метод боротьби з джиттером - джиттер-буфер, який зберігає визначену кількість пакетів.

Зазвичай передбачається динамічне підстроювання довжини буферу протягом всього часу існування з'єднання. Для вибору найкращої довжини використовуються евристичні алгоритми.

Джиттер-буфер

Для компенсації нерівномірної швидкості надходження пакетів на приймальній стороні створюють тимчасове сховище пакетів, або так званий ***джиттер-буфер.*** Його завдання, зібрати пакети, які надходять, у правильній послідовності у відповідності з тимчасовими мітками і видати їх кодеку з правильними інтервалами і правильному порядку.

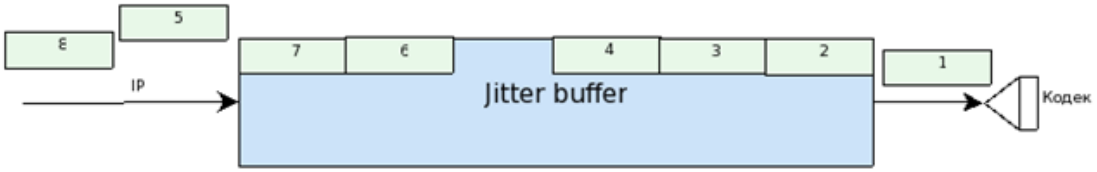

Рис.33. Джиттер-буфер

Розмір буферу приймальний VoIP пристрій розраховує в процесі роботи, або примусово задається у налаштуваннях. З одного боку він не може бути занадто великим, щоб не збільшувати транспортну затримку. З іншого боку, маленький розмір буферу викликає втрати пакетів при змінах часу затримки в IP мережі.

Звідси і відбувається одне з головних протиріч, між інтернет провайдерами та користувачами IP телефонії. З точки зору провайдеру всі пакети доставлені абоненту, тобто, втрат немає. А з точки зору VoIP пристрої, різниця в часі між приходом пакетів значно перевищує джиттер-буфер. Тому фактично втрати є. На практиці втрата більше 1% викликає певні неприємні відчуття. При 2% розмова виявляється затрудненою. При значеннях більше 4% розмова вже практично неможлива.

Розмір джиттер-буферу

Випадкова затримка розповсюдження Ji для і-го пакету може визначатися за формулою:

$$J_i = J_{i-1} + \frac{|D_{i-1}| - J_{i-1}}{16}$$

де:

Di – відхилення від очікуваного часу прибуття і-го пакету. Відхилення від очікуваного часу прибуття і-го пакету Di визначається за формулою:

$$D_i = (R_i - R_{i-1}) - (S_i - S_{i-1})$$

де:

R – час прибуття пакету у мітках часу RTP,

S – часова мітка RTP, яка взята з пакету.

Наведемо приклад розрахунку очікуваного розміру випадкової затримки розповсюдження 5-го пакету, на основі двох попередніх.

Нехай J4=10 мс; R4=10, R3=11, S4=6, S3=5, тоді D5 буде рівним (10-11)-(6-5)= -2.

$$J_5 = 10 + \frac{|-2| - 10}{16} = 9{,}5 \text{ мс}$$

У середньому, випадкова затримка часу розповсюдження для одного пакету в поточному прикладі складе 10 мс (точніше можна порахувати за формулою, наведеною вище). Тоді для того, щоб жоден пакет не був відкинутий, розмір джиттер-буфера повинен бути рівним 10 мс.

Для визначення необхідного розміру джиттер-буфера в мегабайтах, домножимо отримане значення на 100 Мбіт/сек - середню пропускну спроможність мережі: 10•10^-3•100 = 128кб.

Розмір джиттер-буфера повинен бути більше, ніж флуктуація транзитного часу в мережі. Наприклад, якщо для 10 пакетів час транзиту коливається від 5 до 10 мс, то буфер повинен бути хоча б 8 мс, щоб жоден пакет не був втрачений. Краще, якщо буфер ще більше, наприклад, 12 мс, тоді зможе працювати механізм перезапиту втрачених пакетів.

Втрата пакетів

Втрачені пакети в IP-телефонії порушують мову і створюють спотворення тембру. В існуючих IP-мережах усі голосові кадри обробляються як дані. При пікових навантаженнях та перевантаженнях голосові кадри будуть відкидатися, як і кадри даних. Але кадри не пов`язані з часом і відкинуті пакети можуть бути успішно передані шляхом повторення. Втрата голосових пакетів, у свою чергу, не може бути заповнена таким способом і в результаті відбудеться неповне передавання інформації. Передбачається, що втрата до 5% пакетів непомітна, а вище 10-15% - недопустима. Причому дані величини суттєво залежать віл алгоритмів компресії/декомпресії.

Суттєво, що втрата великої групи пакетів призводить до непоправимих локальних спотворень мови, тоді як втрати одного, двох, трьох пакетів можливо

намагатися компенсувати.

Зрозуміло, що із збільшенням трафіку зростають затримки і втрати у телефонному каналі. В умовах обмежених пропускних спроможностей це проявляється не тільки при інтегральному збільшенні завантаження каналів, наприклад, у ГНН, але й при збільшенні потоку локального джерела інформації. Саме тому необхідно використовувати якомога більш низькі швидкості передавання голосової інформації при дійсній вимозі забезпечення потрібної якості телефонного зв'язку.

Відлуння, пристрої обмеження його впливу

Феномен відлуння викликає затруднення під час розмови у обох співрозмовників. У телефонних мережах існують два види відлуння:

1 - відлуння того, хто говорить - коли абонент говорить по телефону і чує власний голос;

2 - відлуння того, хто слухає - коли абонент чує голос співрозмовника двічі.

Відлуння представляє собою проблему у випадку, коли інтервал між моментом, коли абонент говорить, і моментом появи відображеного сигналу стає досить великим.

Існують два види пристроїв, які призначені для обмеження шкідливих ефектів відлуння:

1 - *Ехозагороджувачі* - принцип роботи полягає у відключенні каналу передавання, коли у каналі прийому присутній мовний сигнал.

2 - *Ехокомпенсатори* - більш складний пристрій, який моделює ехо-сигнал для подальшого його віднімання з прийнятого сигналу. Після віднімання синтезованої копії ехо-сигналу із сигналу зворотного напрямку отриманий сигнал підлягає нелінійній обробці для збільшення ступеня подавлення відлуння (подавлення дуже слабких сигналів).

На сьогоднішній день має місце використання більш складних алгоритмів ехокомпенсації, що дозволяє подавляти відлуння, що представляє собою не тільки затриманий, але й здвинутий по частоті сигнал (що часто відбувається із-за наявності в ТМЗК застарілих частотних систем передавання).

Все частіше застосовують алгоритми ехокомпенсації в обладнанні IP-телефонії на базі, наприклад, інтелектуальної платформи.

4.3 Процедури обробки мови в IP-телефонії. Методи кодування голосової інформації

Для забезпечення якісного передавання мовних сигналів в IP-телефонії необхідний їх наступний алгоритм обробки:

1. Усунення всіх небажаних компонентів із вхідного аудіосигналу. Після оцифровки мови необхідно видалити відлуння з динаміка в мікрофон, кімнатне відлуння і безперервний фоновий шум (наприклад, шум від вентилятора), а також відфільтрувати шуми змінного струму на низьких частотах звукового спектру.

Ефективне ехо-подавлення і зменшення шумів абсолютно необхідне у будь-якій конфігурації з «відкритим мікрофоном» і з гучномовцем на базі персонального комп'ютера (ПК) для традиційної і IP-телефонії. Ці функції все в більшій мірі реалізуються аудіокомпонентами ПК, так що сама система IP-телефонії може їх і не мати. Шлюзам IP - телефонії потрібно виконувати менший обсяг попередньої обробки, ніж кінцевим рішенням, тому що УАТС і телефонна мережа забезпечують фільтрацію та зменшення шумів.

2. Подавлення пауз у мові; розпізнавання залишкового фонового шуму (зовнішніх шумів) і кодування для відновлення на дальньому кінці; те ж саме для впізнаваємих сигналів. Паузи найкраще повністю пригнічувати на дальньому кінці. Для збереження оточуючих звуків необхідно змоделювати фонові шуми, щоб система на дальньому кінці могла відновиті їх для слухача. Сигнали багаточастотних набору номеру DTMF та інші сигнали можна замініті на короткі коди для відновлення на дальньому кінці (або для безпосередньої обробки). Можливі проблеми: через те, що функція подавлення пауз активізується, коли гучність мови стає нижче певного порогу, деякі системи обрізають початки та кінці слів (у періоди наростання і зниження енергії мови).

3. Стиснення голосових даних. Стиснути оцифрований голос можна різними способами. В ідеалі рішення, які використовуються для IP телефонії, повинні бути досить швидкими для виконання на недорогих цифрових сигнальних процесорах DSP, зберігати якість мови і давати на виході невеликі масиви даних.

4. «Нарізання» стислих голосових даних на короткі сегменти рівної довжини, їх нумерація по порядку, додавання заголовків пакетів і передавання. Хоча стек протоколів TCP/IP підтримує пакети змінної довжини, їх використання ускладнює досягнення стійкої і передбачуваної міжмережної маршрутизації у голосових додатках. Маршрутизатори швидко обробляють невеликі пакети і розглядають звичайно всі передаваємі по одній і тій же IP-адресі пакети одного розміру однаковим чином. У результаті пакети проходять по одному маршруту, тому їх не потрібно переупорядковувати.

5. Прийом і переупорядкування пакетів в адаптивному «буфері ресинхронізації» для забезпечення інтелектуальної обробки втрат або затримок пакетів. Головною метою тут є подолання впливу змінної затримки між пакетами. Вирішення цієї проблеми полягає у буферизації достатньої кількості пакетів, які надходять (при відкладеному їх відтворенні) з тим, щоб відтворення було безперервним, навіть якщо час між надходженням пакетів сильно відрізняється.

Кращі продукти для IP-телефонії моделюють продуктивність мережі і регулюють розмір буферу ресинхронізації відповідним чином – зменшуючи його (скорочуючи затримку перед відтворенням), коли мережа поводить себе передбачуваним чином, і збільшуючи в протилежному випадку.

Методи кодування голосової інформації

Одним із важливих факторів ефективного використання пропускної спроможності IP-каналу є вибір оптимального алгоритму кодування/ декодування мовної інформації - ***кодеку.***

Всі існуючі на сьогодні типи голосових кодеків за принципом дії можна розділити на три групи:

1. Кодеки з імпульсно-кодовою модуляцією (ІКМ) та адаптивною диференціальною імпульсно-кодовою модуляцією (АДІКМ). У більшості випадків, представляють собою поєднання АЦП/ЦАП.

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

3. Комбіновані (гібридні) кодеки поєднують у 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.34 представлена усереднена суб'єктивна оцінка якості кодування мови для перерахованих типів кодеків.

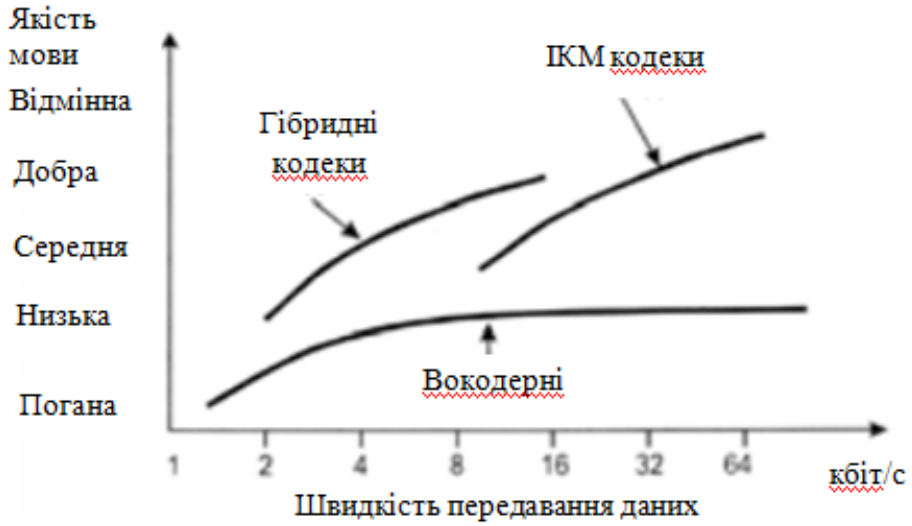

Рис.34. Усереднена суб'єктивна оцінка якості кодування мови для різних типів кодеків

Рис.35. Стандарти для кодування мовних сигналів

Вимоги до алгоритмів кодування сигналу

- Використання смуги пропускання каналу. Швидкість передавання, яку передбачають наявні на сьогодні вузькосмугові кодеки, знаходиться в межах 1.2-64 кбіт/с. Відповідно, що від цього параметра прямо залежить якість відтворної мови.
- Подавлення періодів мовчання. Якщо застосувати алгоритми, які дозволяють зменшити обсяг інформації, що передається в періоди мовчання, то можна значно звузити необхідну смугу пропускання.
- Генератор комфортного шуму (Comfort Noise Generator - CNG) служить для генерації фонового шуму.
- Розмір кадру. Визначає мінімальну теоретично досягаєму затримку передавання інформації (алгоритмічну затримку).
- Чутливість до втрат кадрів. Кодери типу G.723.1 розроблені так, що вони функціонують без істотного погіршення якості в умовах некоррельованих втрат до 3% кадрів, проте при перевищенні цього порогу якість значно погіршується.

Кодеки IP-телефонії

Кодек G.711

Імпульсно кодова модуляція (PCM — Pulse Code Modulation) - передавання неперервної функції у вигляді серії послідовних імпульсів.

При демодуляції послідовність нулів та одиниць перетворюється в імпульси демодулятором, рівень квантування якого дорівнює рівню квантування модулятора. Після цього ЦАП на основі даних імпульсів відновлює сигнал, а згладжуючий фільтр остаточно прибирає неточності.

У сучасній телефонії кількість рівнів квантування має бути більшою або рівною 100, тобто мінімальна кількість біт, яким може кодуватися сигнал - 7.

Кодек G.711 – один з перших цифрових кодеків мовних сигналів, який є мінімально необхідний.

Рекомендація G.711 описує кодек, який використовує ІКМ перетворення аналогового сигналу з точністю 8 біт, тактовою частотою 8 кГц і найпростішої компресією амплітуди сигналу. Швидкість потоку даних на виході перетворювача складає 64 кбіт/с (8 біт х 8 кГц). Для зменшення шуму квантування і покращення перетворення сигналів з невеликою амплітудою при кодуванні використовується нелінійне квантування по рівню відповідно до спеціального псевдо-логарифмічного закону: **А-закон** для європейської системи ІКМ-30/32 або **μ-закон** для північноамериканської системи ІКМ-24.

alaw

alaw або А-закон — алгоритм стискання звукових даних із втратою інформації. В основному використовується на території Європи та Росії.

Для сигналу x перетворення по алгоритму alaw має наступний вигляд:

$$F(x) = \operatorname{sgn}(x) \begin{cases} \frac{A|x|}{1+\ln(A)}, & |x| < \frac{1}{A} \\ \frac{1+\ln(A|x|)}{1+\ln(A)}, & \frac{1}{A} \leq |x| \leq 1, \end{cases}$$

де A — параметр стискання (звичайно приймається рівним 87,7).

ulaw

ulaw або μ-закон — алгоритм стискання звукових даних із втратою інформації. В основному використовується на території Японії та Північної Америки.

Для сигналу x перетворення по алгоритму ulaw має наступний вигляд:

$$F(x) = \operatorname{sgn}(x) \frac{\ln(1+\mu|x|)}{\ln(1+\mu)} \qquad -1 \leqslant x \leqslant 1$$

де μ приймається рівним 255 (8 біт) у стандартах Північної Америки та Японії.

Кодек G.711 широко розповсюджений у системах традиційної телефонії з комутацією каналів. Незважаючи на те, що рекомендація G.711 у стандарті H.323 є основною і первинною, у шлюзах IP-телефонії даний кодек застосовується рідко через високі вимоги до смуги пропускання і затримкам у каналі передавання. Використання G.711 у системах IP- телефонії обгрунтоване лише у тих випадках, коли потрібно забезпечити максимальну якість кодування мовної інформації при невеликій кількості одночасних розмов. Одним із прикладів застосування кодеку G.711 можуть послужити IP - телефони компанії Cisco.

Кодек G.723.1

Рекомендація G.723.1 описує гібридні кодеки, що використовують технологію кодування мовної інформації, яка скорочено називається - MP-MLQ (Multy-Pulse - Multy Level Quantization - множинна імпульсна, багаторівнева квантизація), дані кодеки можна охарактеризувати, як комбінацію АЦП/ЦАП і вокодера. Своїм виникненням гібридні кодеки зобов'язані системам мобільного зв'язку. Застосування вокодеру дозволяє знизити швидкість передавання даних у каналі, що принципово важливо для ефективного використання радіотракту та IP-каналу. Основний принцип роботи вокодеру - синтез вихідного мовного сигналу за допомогою адаптивної заміни його гармонійних складових набором частотних фонем і узгодженими шумовими коефіцієнтами.

Кодек G.723 здійснює перетворення аналогового сигналу у потік даних із швидкістю 64 кбіт/с (ІКМ), а потім за допомогою багатосмугового цифрового фільтру/вокодеру виділяє частотні фонеми, аналізує їх і передає по IP-каналу інформацію тільки про поточний стан фонем у мовному сигналі. Даний алгоритм перетворення дозволяє зменшити швидкість кодованої інформації до 5,3-6,3 кбіт/с без наявного погіршення якості мови. Кодек має дві швидкості і два варіанти кодування: 6,3 кбіт/с з алгоритмом MP-MLQ та 5,3 кбіт/с з алгоритмом CELP. Режим роботи може змінюватися динамічно від кадру до кадру. Перший варіант призначений для мереж з пакетним передаванням голосу і забезпечує кращу якість кодування у порівнянні з варіантом CELP, але менш адаптований до використання у 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 у голосових шлюзах та інших пристроях IP-телефонії. Кодек поступається по якості кодування мови кодеку G.729a, але менш вимогливий до ресурсів процесору та пропускної спроможності каналу.

Кодек G.726

Один із найстаріших алгоритмів стиснення мови ADPCM - адаптивна диференціальна ІКМ (стандарт G.726). Цей алгоритм дає практично таку ж якість відтворення мови, як і ІКМ, але для передавання інформації при його використанні потрібна смуга всього в 16-32 кбіт/с. Метод заснований на тому, що в аналоговому сигналі, який передає мову, неможливі різкі скачки інтенсивності. Тому, якщо кодувати не саму амплітуду сигналу, а її зміну у порівнянні з попереднім значенням, можна обійтися меншою кількістю розрядів. У ADPCM зміна рівня сигналу кодується чотирирьохрозрядним числом, при цьому частота вимірювання 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 разом із кодеком G.711 для зменшення

швидкості кодування останнього. Кодек призначений для використання в системах відеоконференцій.

Кодек G.726 забезпечує кодування цифрового потоку із швидкістю 40, 32, 24 або 16 кбіт/с. Але у додатках IP-телефонії цей кодек практично не використовується, так як він не забезпечує достатньої стійкості до втрат інформації.

Кодек G.728

Гібридний кодек відноситься до категорії LD-CELP – Low Delay – Code Excited Linear Prediction – кодек з управляємим лінійним передбаченням та малою затримкою. Кодек забезпечує швидкість перетворення 16 кбіт/с, вносить затримки при кодуванні від 3 до 5 мс і для реалізації необхідний процесор із швидкодією 40 MIPS. Кодек призначений для використання, в основному, у системах відеоконференцій. У пристроях IP-телефонії даний кодек використовується досить рідко.

Кодек G.728 спеціально розроблявся для обладнання ущільнення телефонних каналів, при цьому була необхідність забезпечити малу величину затримки (менше 5 мс), щоб виключити необхідність застосування ехокомпенсаторів.

Кодек 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 – сполучена структура з управляємим алгербраїчним кодом лінійним передбаченням. Процес перетворення використовує DSP 21,5 MIPS і вносить затримку 15 мс. Швидкість кодованого мовного сигналу складає 8 кбіт/с. У пристроях VoIP даний кодек займає лідируюче положення, забезпечуючи найкращу якість кодування мовної інформації при досить високій компресії.

Кодек G.729 дуже популярний у додатках передавання мови по мережам Frame Relay. Кодек використовує кадр тривалістю 10 мс і забезпечує швидкість передавання 8 кбіт/с. Але для кодеру необхідний попередній аналіз сигналу тривалістю 5 мс.

Існують два різновиди кодеку:

- G.729;
- спрощений варіант G.729A.

Основні характеристики розглянутих кодеків приведені у табл.2.

Табл.2. Характеристики кодеків

Кодек	Метод компресії	Швидкість кодування	Складність реалізації	Якість	Затримка
G.726	ADPCM	32/ 24/ 16 кбит/с	Низька (8 MIPS)	Хороша (32 К), погане (16 К)	Дуже низька (0,125 мс)
G.729	CS-ACELP	8 кбит/с	Висока (30 MIPS)	Хороша	Низька (Юма)
G.729A	CA-ACELP	8 кбит/с	Помірна (20 MIPS)	Середня	Низька (Юма)
G.723.1	MP-MLQ	6,4/5,3 кбит/с	Помірна (16 MIPS)	Хороша (6,4), середня (5,3)	Висока (37 мс)
G.728	LD-CELP	16 кбит/с	Дуже висока (40 MIPS)	Хороша	Дуже низька (3-5 мс)

Додаткова обробка мови завжди призводить до подальшої втрати якості. Тому для якісного передавання мови процедуру компресії/декомпресії бажано застосовувати в мережі тільки один раз. У деяких країнах це є обов'язковою вимогою органів регулювання по відношенню до корпоративних мереж, які підключені до PSTN.

Кількісними характеристиками погіршення якості мови є одиниці ***QDU*** (Quantization Distortion Units): 1 QDU відповідає погіршенню якості при оцифровці з використанням стандартної процедури ІКМ.

Метод компресії	QDU
ADPCM 32 кбит/с	3,5
ADPCM 24 кбит/с	7
LD-CELP 16 кбит/с	3,5
CS-CELP 8 кбит/с	3,5

Згідно рекомендаціям МСЕ-Т, для міжнародних викликів величина QDU не повинна перевищувати 14.

4.4 Комплексна оцінка якості IP-телефонії

Спотворення від компресії/декомпресії оцінюють шляхом опитування різних груп людей за п'ятибальною шкалою одиницями суб'єктивної оцінки MOS (Mean Opinion Score). Оцінки інтерпретують наступним чином:

- 4-5 – висока якість; аналогічна якості передавання голосу в ISDN, або ще вище;
- 3,5-4 – якість ТМЗК (toll quality); така якість звичайно забезпечується більшістю телефонних розмов. Мобільні мережі забезпечують якість трохи нижче, ніж toll quality;
- 3-3,5 – якість мови задовільна, але її погіршення помітне на слух;
- 2,5-3 – мова розбірлива, але вимагає концентрації уваги для розуміння. Така якість звичайно забезпечується у системах зв'язку спеціального призначення (наприклад, у збройних силах).

Для передавання мови з хорошою якістю доцільно орієнтуватися на MOS не нижче 3,5 балів. Значення MOS для різних стандартів кодерів приведене у табл.3.

Табл.3. Середні суб'єктивні оцінки якості різних методів кодування

Кодек	Швидкість передачі, кбіт/с	MOS	Розмір кадру, мс
G.711 PCM	64	4,3	0,125
G.726 Multi-rate ADPCM	16-40	2-4,3	0,125
G.723 MP-MLQ ACELP	5,3; 6,3	3,7; 3,8	30
G.728 LD-CEL	16	4,1	0,625
G.729 CS-ACELP	8	4,0	10
G.729a CS-ACELP	8	3,4	10
GSM RPE-LPC	13	3,9	30

Незважаючи на велику різноманітність, що характеризується пропускними спроможностями, кількістю маршрутизаторів, характеристиками фізичних ліній та іншими характеристиками, реально діючі канали Інтернет характеризуються наступними параметрами:

• дійсною пропускною спроможністю, яка визначається найбільш «вузьким місцем» у віртуальному каналі на даний момент часу;

• трафіком, який також є функцією часу;

• затримкою пакетів, що визначається трафіком, кількістю маршрутизаторів, реальними фізичними властивостями каналів передавання, що утворюють в даний момент часу віртуальний канал, затримками на обробку сигналів, які виникають у голосових кодексах та інших пристроях шлюзів; все це також забезпечує залежність затримки від часу;

• втратою пакетів, яка обумовлена наявністю «вузьких місць», чергами;

• переставлянням пакетів, які прийшли різними шляхами.

Забезпечення якості IP-телефонії на базі протоколу RSVP

Одним із засобів забезпечення якості IP-телефонії і особливо Інтернет-телефонії є використання протоколу резервування ресурсів (Resource Reservation Protocol, RSVP), рекомендованого комітетом IETF. За допомогою RSVP мультимедіа-програми можуть вимагати спеціальної якості обслуговування (specific quality of service, QoS) за допомогою будь-якого з існуючих мережних протоколів - головним чином IP, хоча можливо використовувати й UDP - щоб забезпечити якісне передавання відео- та аудіосигналів. Протокол RSVP передбачає гарантовану QoS завдяки тому, що через кожний комп'ютер, або вузол, який пов'язує між собою учасників телефонної розмови, може передаватися певна кількість даних.

Протокол RSVP призначений тільки для резервування частини пропускної спроможності. Використовуючи RSVP, відправник періодично інформує отримувача про вільну кількість ресурсів повідомленням RSVP Path (рис.36). Транзитні маршрутизатори по мірі проходження цього повідомлення також

аналізують кількість вільних ресурсів, яка є в них, і підтверджують її відповідним повідомленням RSVP Resv, що передається у зворотньому напрямку. Якщо ресурсів достатньо, відправник починає передавання. Якщо ресурсів недостатньо, отримувач повинен зменшити вимоги або припинити передавання інформації.

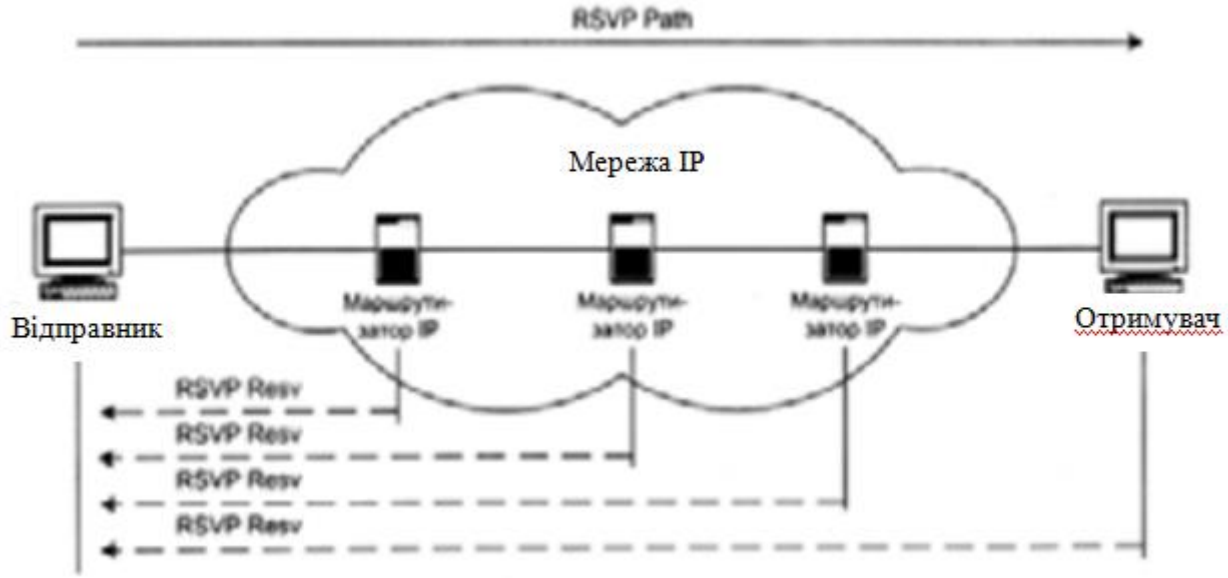

Рис.36. Застосування протоколу RSVP

Однією з цікавих особливостей RSVP є те, що запити на резервування ресурсів направляються тільки від одержувачів даних відправникам, а не навпаки. Такий підхід обумовлений тим, що лише пристрій-одержувач знає, з якою швидкістю він повинен отримувати дані, щоб надійно декодувати аудіо- або відеосигнали. Інша унікальна особливість RSVP полягає в тому, що резервування проводиться лише для одного напрямку. Крім того, RSVP не допускає змішування аудіо- та відеосигналів на зарезервованому каналі.

Коли RSVP-програми закінчать сеанс зв'язку, вони повинні викликати функцію скасування, передбачену цим протоколом. Скасування анулює всі запити на ресурси, зроблені програмою, і дозволяє іншим прикладним програмам використовувати комунікаційні можливості Internet. Якщо програмі не вдається виконати скасування, то передбачені протоколом засоби по закінченню певного проміжку часу виявлять це і автоматично відмінять запит на ресурси.

Забезпечення якості IP-телефонії на базі протоколів RTP та RTCP

Для зменшення значень джиттера і затримок на мережному рівні використовуються механізми RSVP, MPLS, Diff-Serv, які гарантують користувачу заданий рівень якості. Вони покращують якість послуг, що надаються мережею, але не можуть повністю усунути утворення черг у мережних пристроях, а, отже , і зовсім прибрати джиттер. Компенсувати його негативний вплив дозволяє розроблений IETF протокол прикладного рівня RTP (Real-time Transport Protocol),

який використовується технологіями H.323 і SIP.

Протокол RTP (RFC 1889) призначений для доставки чутливої до затримок інформації з використанням мережних служб одноадресної або групової розсилки. Він не має власних механізмів, що гарантують своєчасну доставку пакетів або інші параметри якості послуг - це здійснюють нижчестоячі протоколи. Він навіть не забезпечує всі ті функції, які зазвичай надають транспортні протоколи, зокрема, функції щодо виправлення помилок або управління потоком. Звичайно RTP працює поверх UDP і використовує його служби, але може функціонувати і поверх інших транспортних протоколів (рис.37).

Служба RTP передбачає зазначення типу корисного навантаження і послідовного номеру пакета в потоці, а також застосування тимчасових міток. Відправник позначає кожний RTP-пакет тимчасовою міткою, а одержувач витягує її й обчислює сумарну затримку. Різниця в затримці пакетів дозволяє визначити джиттер і пом'якшити його вплив - всі пакети будуть видаватися додатку з однаковою затримкою.

Таким чином, головна особливість RTP - це обчислення середньої затримки деякого набору прийнятих пакетів і видавання їх додатку користувача з постійною затримкою, що дорівнює цьому середньому значенню.

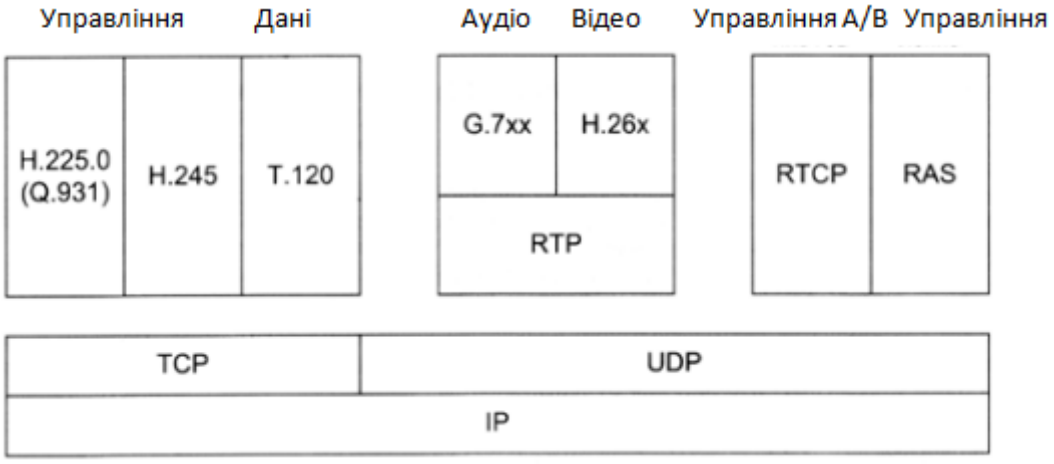

Рис.37. Стек протоколів H.323

Ще одна перевага RTP полягає в тому, що його можна використовувати з RSVP для передавання синхронізованої мультимедіаінформації з певним рівнем якості обслуговування. Крім того, розмови передаються по мережі Internet в незашифрованому вигляді. Тому будь-який вузол, який знаходиться на шляху прямування даних, може підключитися до цієї лінії і прослухати нашу розмову.

Можливості RTP можна розширити, об’єднавши його ще з одним протоколом IETF, а саме з протоколом управління передаванням у реальному часі (Real-time Transport Control Protocol, RTCP). За допомогою RTCP контролюється доставка RTP-пакетів і забезпечується зворотній зв'язок з передавальною стороною та

іншими учасниками сеансу. RTCP періодично розсилає свої управляючі пакети, використовуючи той самий механізм розподілу, який застосовується й для RTP-пакетів з інформацією користувачів.

Основною функцією RTCP є організація зворотного зв'язку з додатком для звіту в якості інформації, яка отримується. RTCP передає відомості (як від приймача, так і від відправника) про кількість переданих і втрачених пакетів, значенні джиттера, затримки і т.д. Ця інформація може бути використана відправником для зміни параметрів передавання, наприклад, для зменшення коефіцієнта стиснення інформації з метою покращення якості її передавання. RTCP також передбачає ідентифікацію користувачів-учасників сеансу.

Один із способів розширення можливостей RTP полягає у використанні його разом з протоколом RSVP, який офіційно не входить у комплект протоколів H.323, але підтримується багатьма додатками реального часу.

Забезпечення якості IP-телефонії на базі протоколу IPv6

IPv6 включає наступні можливості, які відсутні у IPv4:

• *розширений адресний простір:* IPv6 використовує 128-бітові адреси замість 32-бітових IPv4. В результаті адресний простір збільшується у 2^{96} разів, що явно достатньо навіть в разі неефективного розподілу мережних адрес;

• *покращені можливості маршрутизації*: у зв’язку із збільшенням міжмережного трафіку, який пов’язаний з обробкою великих об’ємів мультимедійної інформації та розширенням використання мережі Інтернет у різних сферах діяльності, суттєвою є необхідність забезпечення високих швидкостей маршрутизації. Без застосування ефективних алгоритмів обробки пакетів даних стає неможливим підвищити швидкості роботи маршрутизаторів до рівня, який порівнюється із швидкостями передавання інформації по каналам зв’язку;

• *управління доставкою інформації:* IPv6 дозволяє відмічати відповідність визначеного пакету певним умовам його передавання, заданим відправником. У результаті досягається регулювання швидкості передавання визначених потоків даних, що дозволяє забезпечувати ефективну підтримку спеціальних протоколів (наприклад, відео в режимі реального часу та ін.). За рахунок призначення пріоритетів передавання даних по визначеним протоколам, з'являється можливість гарантувати першочерговість обробки найбільш критичної інформації та надання важливим даним всієї смуги пропускання каналу зв'язку. Інші особливості, які є у IPv6, дозволяють протоколам цього сімейства забезпечувати одночасну багатоадресну доставку інформації. Дана можливість знаходить своє застосування у розсилці інформації "по підписці" або "на вимогу", а також в інших додатках;

• *засоби забезпечення безпеки:* IPv6 надає можливості захисту від атак, які пов'язані з підміною вихідних адрес пакетів, і від несанкціонованого доступу до полів даних пакетів. Ці можливості досягаються за рахунок застосування алгоритмів аутентифікації та шифрування.

Відповідно, від вузлів з IPv6 потрібне виконання двох властивостей:

- можливість взаємодіяти з IPv4-вузлами;
- можливість передавати пакети IPv6 через існуючу інфраструктуру IPv4.

Щоб виконати ці вимоги, робоча група по переходу на IP нового покоління пропонує два основних методи:

- одночасна підтримка у вузлах (і в хостах, і в маршрутизаторах) IPv6 двох стеків протоколів (IPv6/ IPv4);
- тунелювання пакетів IPv6 для їх передавання через інфраструктуру IPv4.

Забезпечення якості IP-телефонії на базі диференційованого обслуговування

Ще одна технологія QoS розроблена робочою групою IETF по диференційованому обслуговуванню (Differentiated Services, DiffServ). Ця група виділилася з робочої групи по інтегрованому обслуговуванню (Integrated Services, IntServ), задача якої полягає у розробці стандартів для підтримки трафіку Internet реального часу.

Диференційоване обслуговування пропонує більш простий і масштабований метод QoS для додатків реального часу. Одним із ключових моментів в роботі над DiffServ є перевизначення ня 8-бітного поля «Тип сервісу» у заголовку IPv4. Назване «Диференційованим обслуговуванням» (DS), це поле може містити інформацію, на основі якої вузли вздовж маршруту визначають, яким чином їм потрібно обробляти пакети та передавати їх наступному маршрутизатору.

На теперішній час тільки 6 із 8 біт у полі DS були визначені, і тільки одне призначення було стандартизоване. Це призначення відоме як прийняте за замовчуванням -Default (DE), - і воно визначає клас обслуговування по мірі можливості. Інше передбачуване призначення, термінове відправлення (Expedited Forwarding, EF), повинне забезпечити скорочення затримок і втрат пакетів.

При надходженні трафіку у мережу граничний маршрутизатор класифікує трафік у відповідності з інформацією, яка міститься у полі DS. Він передає наступним за ним маршрутизаторам цю інформацію, на основі якої вони дізнаються, яким чином обробляти даний конкретний потік.

DiffServ класифікує потоки у відповідності з передвизначеними правилами і потім об’єднує однотипні потоки. Весь трафік з однаковими мітками розглядається однаковим чином, тому реалізація DiffServ у мережі великого підприємства або по каналам глобальної мережі здається більш реальним завданням.

Як можна здогадатися, переваги DiffServ не можна отримати автоматично. Маршрутизатор повинні розуміти «помічені потоки» і вміти відповідним чином реагувати на них. Це потребує модернізації мікропрограмного забезпечення маршрутизаторів. На щастя, з популярністю DiffServ все більша кількість виробників намагається підтримувати дану архітектуру у майбутніх версіях своїх продуктів.

Забезпечення якості IP-телефонії на базі MPLS

Конкурентом DiffServ на роль протоколу для забезпечення QoS є інший проект IETF під назвою «Багатопротокольна комутація міток» (Multiprotocol Label Switching, MPLS).

Якщо DiffServ задіює заголовок DS, який вже є у пакетах IPv4, то MPLS використовує 32-розрядну інформаційну мітку, яка додається до кожного IP-пакету. Ця мітка, яка додається при вході в мережу з підтримкою MPLS, повідомляє кожному маршрутизатору вздовж шляху прямування, як потрібно обробляти пакет.

На відміну від поля DS, мітка MPLS спочатку не є частиною пакету IP. Швидше, вона додається при надходженні пакету в мережу і видаляється при виході пакету з мережі MPLS.

У звичайній ситуації маршрутизатори аналізують заголовок пакету для визначення його адресату. З огляду на те, що такий аналіз проводиться на кожному транзитному вузлі незалежно, передбачити, яким маршрутом буде прямувати пакет, практично неможливо, тому забезпечення гарантованого рівня QoS виявляється неймовірно складним завданням.

При використанні міток MPLS маршрутизатор або комутатор може привласнити мітки записам із своїх таблиць маршрутизації і у вигляді міток передати інформацію про маршрутизацію визначеним маршрутизаторам і комутаторам. Зрахувавши мітку, кожний комутатор або маршрутизатор дізнається інформацію про наступного адресата на шляху, не аналізуючи заголовок пакету. Це економить час і ресурси ЦПУ. Пакети з мітками MPLS можуть, відповідно, передаватися від відправника до одержувача без затримок на обробку, причому всі проміжні вузли знають, яким чином потрібно обробляти кожний пакет.

На практиці MPLS можна використовувати для доставки IP-трафіку по мережам IP.

Слід зазначити, що DiffServ функціонує на третьому рівні, а MPLS – на другому, тому з технічної точки зору обидві технології можуть мирно існувати одна з одною. Як уже зазначалося, DiffServ класифікує пакети при їх надходженні на крайовий маршрутизатор, тому даний стандарт, швидше за все, буде використовуватися на границі мережі, наприклад, між компанією та її сервіс-

провайдером.

З огляду на те, що MPLS передбачає включення додаткових міток і використання маршрутизаторів/комутаторів, здатних інтерпретувати дану інформацію, він, ймовірно, знайде застосування виключно всередині корпоративних мереж або базової мережі оператора, де потрібний високий рівень QoS для IP-трафіку.

Якщо DiffServ потребує деякого налаштування мережних маршрутизаторів, то MPLS передбачає більш серйозну модернізацію, щоб маршрутизатори могли читати мітки та направляти пакети за визначеними маршрутами.

Кожна з технологій має свої переваги у визначених областях мережі, тому постачальники, скоріш за все, будуть підтримувати їх обидві.

Забезпечення якості IP-телефонії за допомогою механізму управління на основі правил

Одним із перспективних напрямків у реалізації гарантованих рівнів якості сервісу (QoS) в середовищі IP є *технологія управління на основі правил*, яка розробляється на теперішній час.

Набір правил, або стратегія, описує спосіб розподілу ресурсів мережі між її клієнтами - користувачами, додатками або хост-машинами. Виділення цих ресурсів може відбуватися статично і динамічно, в залежності від різних факторів, наприклад, часу дня, обсягу самих вільних ресурсів або наявності у клієнтів підтверджених авторизацією привілеїв.

Високорівневі формулювання стратегії (наприклад, «Надавати пріоритет усім пакетам трафіку voice-over-IP») перетворюються у структурований набір правил виду «якщо <умова>, то <реакція>», який зберігається у базі адміністратора, витягується і інтерпретується різними мережними компонентами.

Один із найбільш багатообіцяючих проектів в області управління мережею на основі правил реалізується на теперішній час IETF: це дослідження, пов'язані з визначенням стандартної інфраструктури для застосування даної методології, а також набору необхідних протоколів і схем роботи. Згідно із вже наявними матеріалами IETF, у складі типової мережі, що адмініструється по набору правил, повинні бути присутніми наступні елементи:

- консоль для задавання стратегій – засіб адміністрування, за допомогою якого мережний адміністратор створює та редагує набір правил управління;
- точка прийняття рішень (policy decision point, PDP) – сервер, який забезпечує вибірку правил із сховища та вироблення рішень;
- точки реалізації стратегій (policy enforcement point, PEP) – різні мережні пристрої (маршрутизатори, комутатори і брандмауери), які втілюють у життя рішення PDP (тобто правила управління мережею) за допомогою списків доступу,

алгоритмів управління чергами та інших засобів;

- сховище стратегій – здатний працювати з протоколом LDAP сервер, на якому у спеціальному каталозі зберігаються стратегії.

Зв’язок між елементами PDP та PEP забезпечує нескладний протокол запитів/відповідей Common Open Policy Service (COPS).

Типова мережа з підтримкою адміністрування на основі стратегій та механізмів забезпечення QoS показана на рис.38.

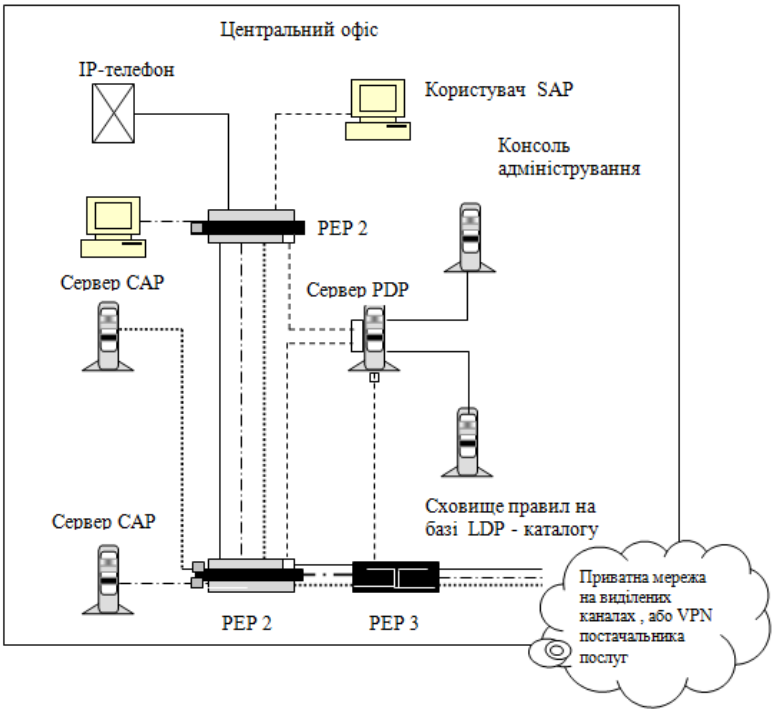

Рис.38. Типова мережа з підтримкою адміністрування на основі стратегій та механізмів забезпечення QoS

Служба каталогів на базі протоколу LDAP

Протокол LDAP (Lightweight Directory Access Protocol - спрощений протокол доступу до каталогів) є стандартом доступу до служб мережних каталогів, а протокол DHCP використовується для динамічного присвоєння IP-адрес користувачам для доступу до мережних ресурсів. Як заявляють компанії-розробники, об'єднання цих двох технологій допоможе вирішити деякі серйозні проблеми, властиві протоколу TCP/IP, наприклад, управління адресами, розробку стратегії безпеки і одночасне використання інформації про адреси (на що не здатні DHCP-сервери).

Протокол LDAP спрощує роботу у мережному середовищі. Так, користувачі отримують можливість входити в систему з будь-якого вузла мережі і працювати із звичними для себе налаштуваннями, оскільки інформація про них буде зберігатися в основаному на LDAP каталозі.

Процес взаємодії серверів LDAP та DHCP показаний на рис.39. Клієнт

надсилає запит на доступ до Інтернет із вказуванням потрібної адреси та ресурсу. Сервер DHCP автоматично присвоює клієнту IP-адресу і зв’язує користувача з ресурсами у каталозі LDAP. Сервер LDAP знаходить вказані ресурси і автоматично з’єднує користувача з відповідним вузлом мережі.

Як і DNS, LDAP - це служба каталогів в архітектурі клієнт-сервер. Каталоги можуть містити найрізноманітнішу інформацію, наприклад, базу даних перерахунку телефонних номерів E.164 в IP-адреси для користувачів IP-телефонії.

Дані, які складають дерево каталогу LDAP, зберігаються на одному або більше серверах LDAP. Якщо при зверненні клієнта LDAP, наприклад, шлюзу IP-телефонії, сервер не може відповісти на запит, то у всякому разі він може повернути йому вказівник на інший сервер LDAP, де запитувана інформація може бути знайдена.

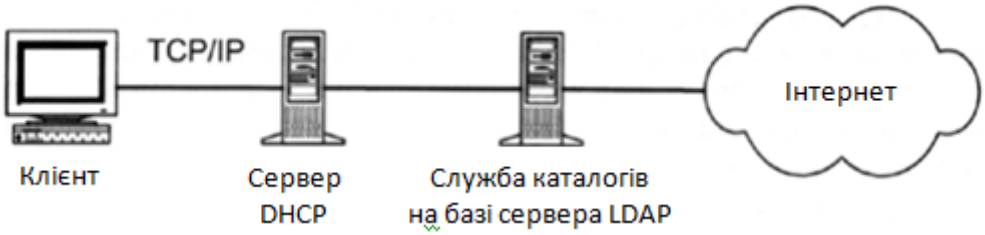

Рис.39. Процес взаємодії серверів DHCP та LDAP

4.5 Інформаційна безпека в мережах IP-телефонії

Види загроз в мережах IP-телефонії:

- *Прослуховування.* У момент передавання конфіденційної інформації про користувачів (ідентифікаторів, паролів) або конфіденційних даних по незахищених каналах існує можливість прослуховування і зловживання ними в корисних цілях зловмисників.
- *Маніпулювання даними.* Дані, які передаються по каналам зв'язку, можна змінити.
- *Підміна даних* про користувача відбувається в разі спроби видачі одного користувача мережі за іншого. При цьому виникає ймовірність несанкціонованого доступу до важливих функцій системи.
- *Відмова в обслуговуванні* (denial of service - DoS) є одною з різновидів атак порушників, в результаті якої відбувається виведення з ладу деяких вузлів або всієї мережі.
    - Вона здійснюється шляхом переповнення системи непотрібним трафіком, на обробку якого надходять всі системні ресурси.
    - Для запобігання цієї небезпеки необхідно використовувати засіб для розпізнавання подібних атак і обмеження їх впливу на мережу.

Особливості системи безпеки в IP-телефонії

Базовими елементами в області безпеки є: аутентифікація; цілісність; активна перевірка.

Під ***аутентифікацією*** розуміють процедуру ідентифікації користувача або кінцевого пристрою (клієнта, сервера, комутатора, маршрутизатора, брандмауера і т.д.).

Використання паролів

- Механізм аутентифікації по протоколу Point-to-Point Protocol (PPP) часто застосовується в середовищі модемного доступу і включає використання протоколів *Password Authentication Protocol (PAP), Challenge Handshake Protocol (CHAP)* і *Extensible Authentication Protocol (EAP).*
- *TACACS* + і *Remote Access Dial-In User Service (RADIUS)* -це протоколи, які підтримують масштабовані рішення в області аутентифікації.
- Протокол *Kerberos* використовується в обмежених областях для підтримки єдиної точки входження в мережу.

- ***Цілісність інформації*** - це здатність засобу обчислювальної техніки або автоматизованої системи забезпечувати незмінність інформації в умовах випадкового і (або) навмисного спотворення (руйнування).
- ***Активна перевірка*** означає перевірку правильності реалізації елементів технології безпеки і допомагає виявляти несанкціоноване проникнення в мережу і атаки типу DoS.

Активна перевірка даних діє як система раннього оповіщення про різні типи неполадок і, отже, дозволяє прийняти попереджувальні заходи, поки не завдано серйозної шкоди.

5. АДРЕСАЦІЯ В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

5.1 Нумерація в телефонних мережах загального користування

В даний час нумерація в мережах загального користування з комутацією каналів, які надають послуги телефону зв'язку (телефонні мережі, мережі ISDN, інтелектуальні мережі, стільникові мережі та ін.), Реалізується відповідно до Рекомендації ITU-T E.164.

Система нумерації таких мереж включає міжнародний і національні плани нумерації.

Кожна телефонна Адміністрація розробляє національний план нумерації для своєї мережі. Цей план розробляється таким чином, щоб будь-який абонент національної мережі може бути доступний по одному і тому ж номеру для різних послуг. Причому це має виконуватися для всіх вхідних міжнародних викликів.

Національний план нумерації країни повинен бути такий, щоб аналіз цифри не перевищував встановлені межі, застосовні до національного (що означає) номеру N(S)N.

Міжнародний номер телекомунікаційної мережі загального користування включає різне число десятичних цифр, об'єднаних у відповідні поля. Структура міжнародного номера телекомунікаційної мережі загального користування показана на рис.40.

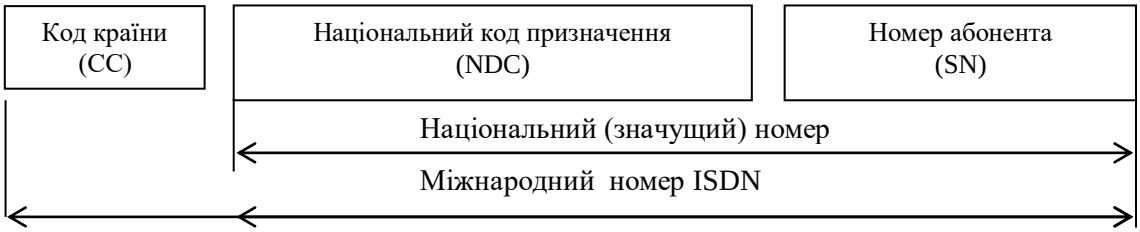

Рис.40. Структура міжнародного номера мережі загального користування

Поле «Код країни (CC)» використовується для визначення країни або географічної області призначення. Даний код має різну довжину, конкретні значення кодів для країн світу наведені в Рекомендації ITU-T E.I64. Слід зазначити, що код країни починається з номера світової зони нумерації. В даний час територія всієї земної кулі поділена на 9 світових зон нумерації:

Зона 1 - Північна Америка;

Зона 2 - Африка;

Зони 3 і 4 - Європа;

Зона 5 - Центральна і Південна Америка;

Зона 6 - Австралія і Океанія;

Зона 7 - Росія і Казахстан;

Зона 8 - Південно-Східна Азія;

Зона 9 - Азія.

Поле «Національний (що означає) номер N (S) N» використовується для визначення конкретного абонента в мережі. При виборі потрібного абонента іноді необхідно визначити ще й мережу призначення. У цьому випадку національний код включає поле національного коду призначення (NDC). Національний код призначення може мати різну довжину в залежності від вимог національних Адміністрацій.

Поле «Номер абонента SN» також має довільну довжину в кожній національній мережі згідно рекомендації ITU-T E.I60.

Слід зазначити, що загальна довжина міжнародного номера в даний час не повинна перевищувати 15 цифр. При цьому в дану довжину номера не входять префікси, символи, адресні обмежувачі (наприклад, закінчення імпульсної сигналів), так як вони не є частиною міжнародного номера мережі загального користування.

5.2 Адресація в IP-мережах

Типи адрес в IP-мережах

Кожен термінал в мережі TCP / IP має адреси трьох рівнів:

1. Фізичний (MAC-адреса) - локальна адреса сайту, який визначається технологією, за допомогою якої побудована окрему мережу, в яку входить даний вузол. Для вузлів, що входять в локальні мережі - це MAC-адреса мережного адаптера або порту маршрутизатора, наприклад, 11-A0-17-3D-BC-01. Ці адреси призначаються виробниками устаткування і є унікальними адресами, так як управляються централізовано. Для всіх існуючих технологій локальних мереж MAC-адреса має формат 6 байтів: старші 3 байти - ідентифікатор фірми виробника, а молодші 3 байти призначаються унікальним чином самим виробником. Для вузлів, що входять в глобальні мережі, включаючи X.25 або frame relay, локальна адреса призначається адміністратором глобальної мережі.

2. Мережевий (IP-адреса), що складається з 4 байт, наприклад, 109.26.17.100. Ця адреса використовується на мережному рівні. Він призначається адміністратором під час конфігурування комп'ютерів і маршрутизаторів. IP-адреса складається з двох частин: номера мережі і номера вузла. Номер мережі може бути обраний адміністратором довільно або назначений за рекомендацією спеціального підрозділу Internet (Network Information Center, NIC), якщо мережа повинна робить як складова частина Internet. Зазвичай провайдери послуг Internet отримують діапазони адрес у підрозділі ний NIC, а потім розподіляють їх між своїми абонентами.

Номер вузла в протоколі IP призначається незалежно від локальної адреси вузла. Розподіл IP-адреси на поле номера мережі і номера вузла - гнучке, і межа між цими полями може встановлюватися досить довільно. Вузол може входити в кілька IP-мереж. В цьому випадку, вузол повинен мати кілька IP-адрес, по числу мережевих зв'язків. Таким чином, IP-адреса характеризує не окремий комп'ютер або маршрутизатор, а одне мережеве з'єднання.

3. Символьний (DNS-ім'я) - ідентифікатор-ім'я, наприклад, SERV1.IBM.COM. Ця електронна адреса призначається адміністратором і складається з декількох частин, наприклад, імені машини, імені організації, імені домену. Така адреса, званий також DNS-ім'ям, використовується на прикладному рівні, наприклад, в протоколах FTP або telnet.

Три основні класи IP-адрес

IP-адреса має довжину 4 байти і звичайно записується у вигляді чотирьох чисел, що представляють значення кожного байта в десятковій формі, і між якими ставлять крапку, наприклад: 128.10.2.30 - традиційна десяткова форма представлення адреси, 10000000 00001010 00000010 00011110 - двійкова форма представлення цього ж адреси. На рис.41 показана структура IP-адреси.

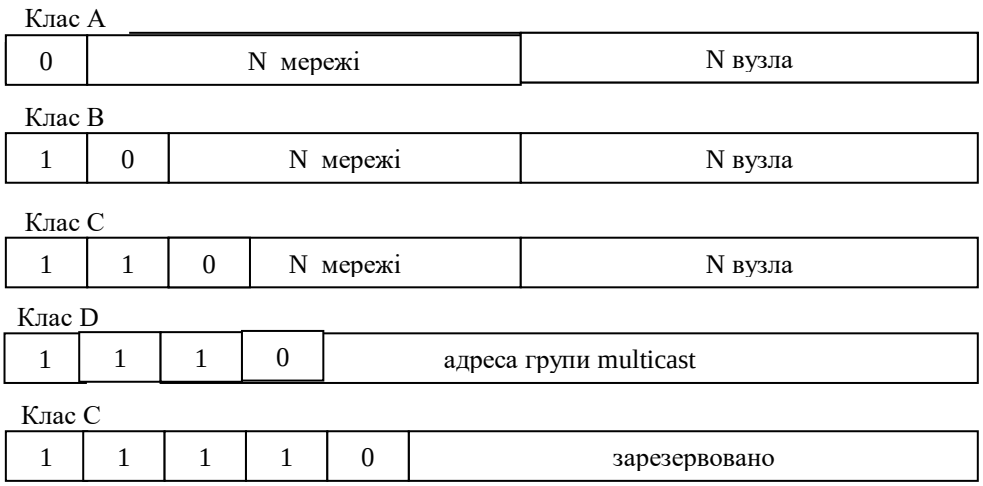

Рис.41. Структура IP-адреси

Адреса складається з двох логічних частин - номера мережі і номера вузла в мережі. Яка частина адреси відноситься до номера мережі, а яка до номера вузла, визначається значеннями перших бітів адреси:

• Якщо адреса починається з 0, то мережу відносять до класу A, і номер мережі займає один байт, інші 3 байти інтерпретірують як номер вузла в мережі. Мережі класу A мають номери в діапазоні від 1 до 126. (Номер 0 не використовується, а номер 127 зарезервований для спеціальних цілей, про що буде сказано нижче.) У мережах класу A кількість вузлів має бути більше 216, але не перевищувати 224.

• Якщо перші два біти адреси рівні 10, то мережа відноситься до класу B і є мережею середніх розмірів з числом вузлів 28-216. У мережах класу B під адресу мережі і під адресу вузла відводиться по 16 бітів, тобто по 2 байти.

• Якщо адреса починається з послідовності 110, то це мережа класу C з числом вузлів не більше 28. Під адреса мережі відводиться 24 біти, а під адреса вузла - 8 бітів.

• Якщо адреса починається з послідовності 1110, то він є адресою класу D і позначає особливий, груповий адрес - multicast. Якщо в пакеті як адреса призначення вказана адреса класу D, то такий пакет повинні получити всі вузли, яким визначено цю адресу.

• Якщо адреса починається з послідовності 11110, то це адреса класу E, він зарезервований для майбутніх застосувань

У табл.4 наведені діапазони номерів мереж, відповідних кожному класу мереж.

Табл.4. Діапазони номерів IP-мереж

Клас	Найменша адреса	Найбільша адреса
A	01.0.0	126.0.0.0
B	128.0.0.0	191.255.0.0
C	192.0.1.0.	223.255.255.0
D	224.0.0.0	239.255.255.255
E	240.0.0.0	247.255.255.255

У протоколі IP-адреса вузла, тобто адреса комп'ютера або порту маршрутизатора, призначається довільно адміністратором мережі і прямо не пов'язаний з його локальною адресою, як це зроблено, наприклад, в протоколі IPX. Підхід, який використовується в IP, зручно використовувати у великих мережах і через його незалежності від формату локальної адреса, і через стабільності, тому що в іншому випадку, при зміні на комп'ютері мережного адаптера ці зміни мали б були враховувати всі адресати всесвітньої мережі Internet (в тому випадку, звичайно, Ерлі мережа підключена до Internet).

Локальний адреса використовується в протоколі IP тільки в межах локальної мережі при обміні даними між маршрутизатором і вузлом цієї мережі. Маршрутизатор, отримавши пакет для вузла однієї з мереж, безпосередньо підключення до його портів, повинен для передачі пакета сформувати кадр відповідно до вимог прийнятої в цій мережі технології і вказати в ньому локальна адреса вузла, наприклад його MAC-адресу. У пакеті, що прийшов цей адреса не вказана, тому перед маршрутизатором постає завдання пошуку його по відомому IP-адресою, яка вказана в пакеті як адреса призначення. З аналогічним завданням зіштовхується й кінцевий вузол, коли він хоче відправити пакет у вилучену мережу через маршрутизатор, підключений до тієї ж локальної мережі, що і цей вузол.

Для визначення локальної адреси по IP-адресою використовується протокол дозволу адреси Address Resolution Protocol, ARP. Протокол ARP працює по-різному залежно від того, який протокол канального рівня працює в даній мережі - протокол локальної мережі (Ethernet, Token Ring, FDDI) з можливістю широкомовного доступу одночасно до всіх вузлів мережі, або ж протокол глобальної мережі (X.25, Frame Relay), як правило, не підтримувати широкомовний доступ. Існує також протокол, що вирішує зворотну задачу - знаходження IP-адреси відомим локального адресою. Він називається реверсивний ARP - RARP (Reverse Address Resolution Protocol) і використовується при старті бездискових станцій, хто знає в початковий момент свого IP-адреси, але знають адресу свого мережного адаптера.

У локальних мережах протокол ARP використовує широкомовні кадри протоколу канального рівня для пошуку в мережі вузла із заданим IP-адресою.

Вузол, якому потрібно виконати відображення IP-адреси на локальний адресу, формує ARP-запит, вкладає його в кадр протоколу канального рівня, вказуючи в ньому відомий IP-адреса, і розсилає запит широковещательно. Всі вузли локальної мережі отримують ARP-запит і порівнюють зазначений там IP-адресу з власним. У разі їх збігу вузол формує ARP-відповідь, в якому вказує свій IP-адресу і свій локальний адресу і відправляє його вже направлено, так як в ARP-запиті відправник вказує свою локальну адресу. ARP-запити і відповіді використовують один і той же формат пакета. Так як локальні адреси можуть у різних типах мереж мати різну довжину, то формат пакета протоколу ARP залежить від типу мережі.

В поле типу мережі для мереж Ethernet вказується значення 1. Поле типу протоколу дозволяє використовувати пакети ARP не тільки для протоколу IP, але і для інших мережевих протоколів. Для IP значення цього поля одно 0800_{16}.

Довжина локальної адреси для протоколу Ethernet дорівнює 6 байтам, а довжина IP-адреси - 4 байтам. В поле операції для АКР запитів вказується значення 1 для протоколу АКР і 2 для протоколу RARP.

Вузол, що відправляє ARP-запит, заповнює в пакеті всі поля, крім поля шуканого локальної адреси (для RARP-запиту не вказується шуканий IP-адреса). Значення цього поля заповнюється вузлом, упізнав свою IP-адресу.

У глобальних мережах адміністратору мережі найчастіше доводиться вручну формувати ARP-таблиці, в яких він задає, наприклад, відповідність IP-адреси адресою вузла мережі X.25, який має сенс локальної адреси. У останнім часом намітилася тенденція автоматизації роботи протоколу ARP і в глобальних мережах. Для цієї мети серед всіх маршрутизаторів, підключених до якої-небудь глобальної мережі, виділяється спеціальний маршрутизатор, який веде ARP-таблицю для всіх інших вузлів і маршрутизаторів цієї мережі. При такому централізованому підході для всіх вузлів і маршрутизаторів вручну потрібно встановити тільки IP-адресу і локальний адреса виділеного маршрутизатора. Потім кожен вузол і маршрутизатор реєструє свої адреси в виділеному маршрутизаторі, а при необхідності встановлення відповідності між IP-адресою і локальною адресою вузол звертається до виділеного маршрутизатору із запитом і автоматично отримує відповідь без участі адміністратора.

Відображення символьних адрес на IP-адреси

Служба DNS (Domain Name System) - це розподілена база даних, що підтримує ієрархічну систему імен для ідентифікації вузлів в мережі Internet. Служба DNS призначена для автоматичного пошуку IP-адреси за відомим символьному імені

вузла. Специфікація DNS визначається стандартами RFC 1034 і 1035. DNS вимагає статичної конфігурації своїх таблиць, що відображають імена комп'ютерів в IP-адресу.

Протокол DNS є службовим протоколом прикладного рівня. Цей протокол несиметричний - в ньому визначені DNS-сервери і DNS-клієнти. DNS-сервери зберігають частина розподіленої бази даних про відповідність символьних імен і IP-адрес. Ця база даних розподілена по адміністративним доменам мережі Internet. Клієнти сервера DNS знають IP-адреса сервера DNS свого адміністративного домену і за протоколом IP передають запит, в ко-тором повідомляють відоме символьне ім'я і просять повернути відповідний йому IP-адреса.

Якщо дані про запрошенням відповідно зберігаються в базі даного DNS-сервера, то він відразу посилає відповідь клієнту, якщо ж ні - то він надсилає запит DNS-сервера іншого домену, який може сам обробити запит або передати його іншому DNS-сервера. Всі DNS-сервери з'єднані ієрархічно, відповідно до ієрархії доменів мережі Internet. Клієнт опитує ці сервери імен, поки не знайде потрібні відображення. Цей процес прискорюється через те, що сервери імен постійно кешують інформацію, що надається за запитами. Комп'ютери клієнтів можуть використовувати в своїй роботі IP-адреси декількох DNS-серверів для підвищення надійності своєї роботи.

База даних DNS має структуру дерева, званого доменним простором імен, в якому кожен домен (вузол дерева) має ім'я і може містити піддомени. Ім'я домену ідентифікує його положення в цій базі даних по відношенню до батьківського домену, причому точки в імені відділяють частини, відповідні вузлам домену.

Корінь бази даних DNS управляється центром Internet Network Information Center. Домени верхнього, рівня призначаються для кожної країни, а також на організаційній основі. Імена цих доменів повинні слідувати міжнародним рідного стандарту ISO 3166. Для позначення країн використовуються трьохбуквені дволітерні абревіатури, а для різних типів організацій використовуються наступні абревіатури:

- com - комерційні організації (наприклад, microsoft.com);
- edu - освітні (наприклад, mit.edu);
- gov - урядові організації (наприклад, nsf.gov);
- org - некомерційні організації (наприклад, fidonet.org);
- net - організації, що підтримують мережі (наприклад, nsf.net).

Кожен домен DNS адміністрірується окремою організацією, яка зазвичай розбиває свій домен на піддомени і передає функції адміністрування цих піддоменів іншим організаціям. Кожен домен має унікальне ім'я, а кожен з піддоменів має унікальне ім'я усередині свого домену. Ім'я домена може містити до 63 символів. Кожен хост в мережі Internet однозначно визначається своїм

повним доменним ім'ям (fully qualified domain name, FQDN), яке включає імена всіх доменів у напрямку від хоста до кореня. Приклад повного DNS-імені: citint.dol.ru.

Автоматизація процесу призначення IP-адрес

Як вже було сказано, IP-адреси можуть призначатися адміністратором мережі вручну. Це являє для адміністратора тяжку процедуру. Ситуація ускладнюється ще тим, що багато користувачів не мають необхідного точними знаннями для того, щоб конфігурувати свої комп'ютери для роботи в інтермережі і повинні тому покладатися на адміністраторів.

Протокол динамічної настройки хоста Dynamic Host Configuration Protocol (DHCP) був розроблений для того, щоб звільнити адміністратора від цих проблем. Основним призначенням DHCP є динамічний призначення IP-адрес. Однак, крім динамічного, DHCP може підтримувати і більш прості способи ручного і автоматичного статичного призначення адрес.

У ручній процедуру призначення адрес активну участь приймає адміністратор, який надає DHCP-серверу інформацію про відповідність IP-адрес фізичним адресами або іншим ідентифікаторів клієнтів. Ці адреси повідомляються клієнтам у відповідь на їх запити до DHCP-сервера.

При автоматичному статичному способі DHCP-сервер привласнює IP-адреса (і, можливо, інші параметри конфігурації клієнта) з пула готівкових IP-адрес без втручання оператора. Межі пулу призначаються адрес задає адміністратор при конфігуруванні DHCP-сервера. Міжідентифікатором клієнта і його IP-адресою, як і раніше, як і при ручному призначення, існує постійну відповідність. Воно встановлюється в момент первічного призначення сервером DHCP IP-адреси клієнта. При всіх наступних запитах сервер повертає той же самий IP-адресу.

При динамічному розподілі адрес DHCP-сервер видає адреса клієнту на обмежений час, що дає можливість згодом повторно використовувати IP-адреси іншими комп'ютерами. Динамічне розділення адрес дозволяє будувати IP-мережу, кількість вузлів в якій набагато перевищує кількість наявних в розпорядженні адміністратора IP-адрес.

DHCP забезпечує надійний і простий спосіб конфігурації мережі TCP / IP, гарантуючи відсутність конфліктів адрес за рахунок централізованого управління їх розподілом. Адміністратор управляє процесом призначення адрес за допомогою параметра «Вартість прокату» (lease duration), яка визначає, як довго комп’ютер може використовувати призначений IP-адреса, перед тим як знову запросити його від сервера DHCP в оренду.

Прикладом роботи протоколу DHCP може служити ситуація, коли комп'ютер, що є клієнтом DHCP, видаляється з підмережі. При цьому призначений йому IP-

адреса автоматично звільняється. Коли комп'ютер підключається до іншої підмережі, то йому автоматично призначається нову адресу. Ні користувач, ні мережевий адміністратор не втручаються в цей процес. Це властивість дуже важливо для мобільних користувачів.

Протокол DHCP використовує модель клієнт-сервер. Під час старту системи комп'ютер-клієнт DHCP, що знаходиться в стані «ініціалізація», посилає повідомлення discover (досліджувати), яке широкомовно поширюється по локальній мережі і передається всім DHCP-серверів приватної інтермережі. Кожен DHCP-сервер, напів чівшій це повідомлення, відповідає на нього повідомленням offer (пропозиція), яке містить IP-адресу і конфігураційну інформацію.

Комп'ютер-клієнт DHCP переходить в стан «вибір» і збирає пропозиції від DHCP-серверів. Потім він вибирає один з цих пропозицій, переходить в стан «запит» і відправляє повідомлення request (запит) тому DHCP-сервера, чиє пропозицію було обрано.

Обраний DHCP-сервер посилає повідомлення DHCP-acknowledgment (підтвердження), що містить той же IP-адреса, який вже був посланий раніше на стадії дослідження, а також параметр оренди для цієї адреси. Крім того, DHCP-сервер посилає параметри мережевої конфігурації. Після того, як клієнт отримає це підтвердження, він переходить в стан «зв'язок», перебуваючи в якому він може брати участь у роботі мережі TCP/IP.

Комп’ютери-клієнти, які мають локальні диски, зберігають отриманий адресу для використання при наступних стартах системи. При наближенні моменту закінчення, терміну оренди адреси комп'ютер намагається оновити параметри оренди у DHCP-сервера, а якщо цей IP-адреса не може бути виділений знову, то йому повертається інший IP-адресу.

У протоколі DHCP описується кілька типів, які використовуються для виявлення і вибору DHCP-серверів, для запитів інформації про конфігурацію, для продовження та дострокового припинення ліцензії на IP-адресу. Всі ці операції спрямовані на те, щоб звільнити адміністратора мережі від утомливих рутинних операцій по конфігурації мережі.

Однак використання DHCP несе в собі і деякі проблеми. По-перше, це проблема узгодження інформаційної адресної бази в службах DHCP і DNS. Як відомо, DNS служить для перетворення символьних імен в IP-адреси. Якщо IP-адреси будуть динамічно змінятся сервером DHCP, то ці зміни необхідно також динамічно вносити в базу даних сервера DNS. Хоча протокол динамічної взаємодії між службами DNS і DHCP вже реалізований деякими фірмами (так звана служба Dynamic DNS), стандарт на нього поки не прийнятий.

По-друге, нестабільність IP-адрес ускладнює процес управління мережею.

Системи управління, засновані на протоколі SNMP, розроблені з розрахунком на статичність IP-адрес. Аналогічні проблеми виникають і при конфігуруванні фільтрів маршрутизаторів, які оперують з IP-адресами.

Нарешті, централізація процедури призначення адрес знижує надійність системи: при відмові DHCP- сервера всі його клієнти виявляються не в змозі отримати IP-адресу та іншу інформацію про конфігурацію. Наслідки такої відмови можуть бути зменшені шляхом використанні в мережі декількох серверів DHCP, кожен з яких має свій пул IP-адрес.

Служба каталогів на базі протоколу LDAP

Протокол LDAP (Lightweight Directory Access Protocol - спрощений протокол доступу до каталогів) є стандартом доступу до служб мережевих каталогів, а протокол DHCP використовується для динамічного присвоєння IP- адрес користувачам для доступу до мережевих ресурсів. Як заявляють компанії-розробники, об'єднання цих двох технологій допоможе вирішити деякі серйозні проблеми, властиві протоколу TCP/IP, наприклад, управління адресами, розробку стратегії безпеки і одночасне використання інформації про адреси (на що не здатного DHCP-сервери).

Протокол LDAP спрощує роботу в мережевому середовищі. Так, користувачі отримують можливість входити в систему з будь-якого вузла мережі і працювати зі звичними для себе настройками, оскільки інформація про них буде зберігатися в заснованому на LDAP каталозі. В майбутньому засновані на LDAP каталоги можуть застосовуватися для підтримки інфраструктури інтрамереж і Internet. Наприклад, служби типу системи іменування доменів (DNS) і DHCP будуть використовувати сервери каталогів на базі LDAP як своїх сховищ інформації. Тоді ці служби придбають додатково тільні гідності - модульну структуру і незалежність від місця розміщення.

Протокол LDAP спеціально призначений для використання з керуючими і браузерних додатками, які забезпечують інтерактивний доступ до каталогів з можливістю читання і запису. LDAP - це протокол взаємодії клієнта і сервера, що забезпечує доступ до служби каталогів і працює безпосередньо над протоколом TCP / IP.

Набір API-інтерфейсів протоколу LDAP досить простий. Протокол стає одним з найбільш предпочтітельних для роботи з каталогами в Internet. Оскільки вже більше 40 компаній забезпечують підтримку LDAP в своїх продуктах або заявили про такий намір, цей протокол швидко завойовує собі популярність і отримує все більш широке поширення. В даний час сервери LDAP випускаються компаніями Microsoft, Netscape Communications, Lucent Technologies, ISODE, Critical Angle, Novell, Banyan Systems та ін. Деякі браузери Web, наприклад Netscape

Communicator, мають вбудований клієнт LDAP.

Застосовувана в LDAP інформаційна модель заснована на схемі, використаної в протоколі X.500, яка, в свою чергу, базується на «іменних записах». Іменні записи позначають або реальні об'єкти, наприклад ка кого-небудь користувача, або деяку мережеву службу, наприклад службу перетворення адрес. Кожен запис супроводжується атрибутами, що мають одне або кілька значень, і зберігає інформацію, яку при необхідності можна знайти. Як правило, каталог на базі LDAP підтримує реплікацію, що підвищує надійність і збільшує швидкодію системи.

Система іменування доменів (DNS) потрібна для того, щоб комп'ютери могли знаходити один одного в мережі. За допомогою комунікаційних протоколів служба DHCP поширює інформацію про IP-адреси та інші відомості серед клієнтів мережі; зазвичай це робиться при запуску системи. Службу DHCP можна налаштувати таким чином, щоб тимчасово привласнювати клієнтам динамічні адреси з деякого банку вільних адрес і перепризначувати ці адреси в міру необхідності.

Автоматичне привласнення IP-адреси вимагає щодо тісного зв'язку між серверами DNS і DHCP, установлене на даному вузлі мережі. Цей зв'язок необхідна, оскільки, присвоюючи клієнту IP-адреса, сервер DHCP повинен мати можливість оновлення інформації про відповідність імені клієнта наданим йому адресою.

Поєднання технологій DHCP і DNS з можливостями каталогів на базі LDAP дозволить домогтися як мінімум наступних переваг:

• доступ до інформації - нова система дозволить організувати стандартний метод доступу для пошуку і збереженні-вати даних в інформаційному сховищі серверів DHCP і DNS;

• гнучкість побудови мережі - оскільки мережевий протокол LDAP здатний працювати на різних платформах, з'являється можливість розміщення серверного сховища інформації на інших машинах;

• реплікація - вже зараз багато постачальників вбудовують функції реплікації в створювані ними служби каталогів на базі LDAP; в майбутньому вони ще більше розширяться, так як комітет IETF починає розробляти стандартний протокол LDAP з можливістю реплікації.

Головна мета об'єднання серверів - дати користувачам можливість вбудовувати в їх системи управління мережними адресами засоби підвищення надійності, безпеки і синхронізації імен та адрес.

Процес взаємодії серверів LDAP і DHCP показаний на рис.42. Клієнт посилає запит на доступ в Internet із зазначенням потрібної адреси і ресурсу. Сервер DHCP автоматично присвоює клієнту IP-адреса і пов'язує користувача з ресурсами в

каталозі LDAP. Сервер LDAP знаходить зазначені ресурси і автоматично з'єднує користувача з відповідним вузлом мережі.

Як і DNS, LDAP - це служба каталогів в архітектурі клієнт-сервер. Каталоги можуть містити саму різну інформацію, наприклад, базу даних перерахунку телефонних номерів E.164 в IP-адреси для користувачів IP- телефонії. Складові дерево каталогу LDAP дані зберігаються на одному або більше серверах LDAP. Якщо при звертанні клієнта LDAP, наприклад шлюзу IP-телефонії, сервер не може відповісти на запит, то у всякому разі він може повернути йому покажчик на інший сервер LDAP, де запитувана інформація може бути знайдена.

Рис.42. Процес взаємодії серверів DHCP та LDAP

Адресація в IPv6

Одним з основних відмінностей впроваджуваного в даний час протоколу IPv6 від протоколу IPv4 є ис користування довших адрес. Адреси одержувача і джерела в IPv6 мають довжину 128 біт або 16 байт. Версія 6 узагальнює спеціальні типи адрес версії 4 в наступних типах адрес:

• Unicast - індивідуальний адресу. Визначає окремий вузол - комп'ютер або порт маршрутизатора. Пакет повинен бути доставлений вузла за найкоротшим маршрутом.

• Cluster - адрес кластера. Позначає групу вузлів, які мають загальний адресний префікс (напри-мер, приєднаних до однієї фізичної мережі). Пакет повинен бути маршрутизований групі вузлів за найкоротшим шляхом, а потім доставлений тільки одному з членів групи (наприклад, найближчого вузла).

• Multicast - адреса набору вузлів, можливо в різних фізичних мережах. Копії пакету повинні бути доставлені кожному вузлу набору, використовуючи апаратні можливості групової або широкомовної доставки, якщо це можливо.

Як і у версії IPv4, адреси у версії IPv6 поділяються на класи, в залежності від значення декількох старших біт адреси.

Велика частина класів зарезервована для майбутнього застосування. Найбільш цікавим для практичного використання є клас, призначений для провайдерів послуг Internet, названий Provider-Assigned Unicast.

Адреса цього класу має наступну структуру:

010	Ідентифікатор провайдера	Ідентифікатор абонента	Ідентифікатор підмережі	Ідентифікатор вузла

Кожному провайдеру послуг Internet призначається унікальний ідентифікатор, яким позначаються всі мережі, що їм піддержуються. Далі провайдер призначає своїм абонентам унікальні ідентифікатори і використовує обидва ідентіфікатора при призначенні блоку адрес абонента. Абонент сам призначає унікальні ідентифікатори своїм підмережам вузлів цих мереж.

Абонент може використовувати техніку підмереж, яка застосовується в версії IPv4, для подальшого розподілу поля ідентифікатора підмережі на більш дрібні поля.

Описана схема наближає схему адресації IPv6 до схем, які використовуються в територіальних мережах, включаю телефонні мережі або мережі X.25. Ієрархія адресних полів дозволить магістральним маршрутизаторам працювати тільки зі старшими частинами адреси, залишаючи обробку менш значущих полів маршрутизаторам абонентів.

Під поле ідентифікатора вузла потрібно виділення не менше 6 байт, для того щоб можна було використовувати в IP-адреси MAC-адреси локальних мереж безпосередньо.

Для забезпечення сумісності зі схемою адресації версії IPv4, у версії IPv6 є клас адрес, що мають 0000 0000 в старших бітах адреси. Молодші 4 байта адреси цього класу повинні містити адресу IPv4. Маршрутизатор, що підтримують обидві версії адрес, повинні забезпечувати трансляцію при передачі пакету з мережі, що підтримує адресацію IPv4, в мережу, яка підтримує адресацію IPv6, і навпаки.

5.3. Проблеми адресації в мережах IP-телефонії

У системах IP-телефонії, так само як і в мережах з комутацією каналів, номери відповідно до Рекомендації E.164 використовуються кінцевими користувачами, щоб ідентифікувати виклик. У IP-системах, коли кінцевий користувач ідентифікується терміналом, номер E.164 цього кінцевого користувача тимчасово пов'язаний з адресою IP (транспортний адресу) цього терміналу (кінцевої точки). Проблема нумерації в мережі IP-телефонії пов'язана з визначенням точки призначення виклику при внутрідоменной і междоменной зв'язку в IP-мережі. В якості такої кінцевої точки може виступати або IP-термінал з відповідним додатком користувача або шлюз для доступу в мережу з комутацією каналів.

Від вирішення завдань адресації в IP-телефонії в чому залежать зручність

користування послугою, робота алгоритмів маршрутизації, забезпечення мобільності номерів і т.д. Головна проблема організації взаємодії мереж з комутацією каналів і IP-мереж полягає в тому, що єдиний метод адресації звичайного терміналу абонента телефонної мережі - це використання номера цього терміналу (в мережах загального користування номера E.164). Питання пре-освіти номера мережі з комутацією каналів в IP-адреса представляється поки ще досить складним і розробляється не тільки робочою групою 4 в рамках проекту TIPHON, а й іншими організаціями, наприклад IETF. У той же час ITU-T тільки підходить до вирішення питань взаємодії послуг IP-телефонії і PSTN, обмежуючись поки розглядом функцій міжмережевого взаємодії на рівні, транспортних технологій. Така позиція пояснюється, зокрема, відсутністю загальних для всіх національних адміністрацій зв'язку підходів до визначення статусу послуги IP-телефонії.

Оператору IP-телефонії, що пропонує свої послуги абонентам мереж з комутацією каналів, необхідно, природно, використовувати вже наявні схеми нумерації. Згідно з рекомендаціями TIPHON, для організації викликів від абонентів мереж з комутацією каналів користувачам IP-мережі бажано, щоб останні мали номер E.164. У проекті TIPHON також досліджується можливість використання в Інтернет коду країни та коду послуги, які будуть задіяні в Інтернет-телефонії.

У мережах IP-телефонії, побудованих на базі стандарту H.323, перетворення телефонних номерів E.164 в IP- адреси і назад входить у функції gatekeeper. У системах, що використовують протокол SIP, ці функції виконуються в спеціальному сервері.

Табл.5 показує відносини між іменами та адресами для телефонних мереж і додатків Інтернет. Вона також включає відмінності в адресації між концепцією TIPHON і рішеннями по Інтернет-телефонії, що ґрунтуються на протоколі SIP.

Мета перетворення номера - заміна цифр, набраних викликає користувачем, в імена E.164 і перетворити цих імен в адреси, імена або ідентифікатори, які необхідно використовувати для маршрутизації IP- повідомлень управління телефонними викликами. При цьому телефонні з'єднання встановлюються всередині домену або між доменами і / або далі маршрутизуються в мережу з комутацією каналів. Для виконання функцій маршрутизації при обслуговуванні викликів необхідно мати базу даних про користувачів і шлюзах, про перетворення номерів, імен і адрес.

Табл.5. Відносини між іменами та адресами для телефонних мереж і додатків Інтернет

	Телефоні або інші мережі с комутацією каналів	**E-mail**	**Концепція TIPHON**	**Рішення на базі протоколу SIP**
Ім'я	Номер Е.164	user@host где host - ім'я домену	Номер Е.164	user@host, можливо з підстановочним номером Е.164 для вхідних викликів з мереж з комутацією каналів
Адреса	Маршрутизація за номером Е.164 (або префікс маршру-тизації + номер Е.164)	IP-адреса	IP-адреса	IP-адреса

Мережі IP-телефонії повинні підтримати перетворення номерів в двох випадках:

1. Маршрутизовані виклики направляються в мережу з комутацією каналів. У цьому випадку необхідний, по крайней мере, один маршрут до домену, в якому розташований шлюз до мережі з комутацією каналів, що забезпечує доступ до адресата. Хоча можуть бути доступні більш ніж один маршрут, так як кілька доменів і кілька шлюзів дозволяють обслужити цей виклик.

2. Маршрутизовані виклики направляються в мережу з комутацією пакетів (IP-мережу). В цьому випадку викликає користувач використовує номер ЕЛ 64 як назва, яка ідентифікує адресата IP-мережі. При цьому можливий тільки один маршрут через відповідний шлюз. Відповідно до концепції TIPHON мережі IP-телефонії повинні підтримувати, принаймні, одну з на- дмуть схем нумерації:

1. Домени мережі IP-телефонії повинні підтримати всі схеми нумерації на мережах зв'язку з комутацією каналів і забезпечувати належне меж мережева взаємодія з ними.

2. План нумерації для користувачів мереж IP-телефонії може бути таким же, як і для користувачів мереж з комутацією каналів, причому з урахуванням національних особливостей.

3. Нумерація для надання послуг користувачам IP-телефонії повинна бути аналогічною нумерації, що використовується в мережах з комутацією каналів.

Система нумерації IP-телефонії повинна забезпечувати можливість заміни одного номера Е.164 на інший.

Це необхідно для забезпечення підтримки таких послуг:

• мобільність номера;

• персональна нумерація;

• негеографіческой послуги типу freephone.

При таких послугах номер надсилається у вигляді запиту на шлюз IP-телефонії

та ідентифікується як номер маршрутування E.164. Відповідь на запит буде завжди у вигляді номера E.164.

В системі IP-телефонії може існувати два види планів нумерації: відкритий (внутрішній і міжнародний) і приватний. При цьому можливі три формату номерів:

1. Фіксований - набирається номер фіксований;

2. Змінний - набирається номер може змінюватися;

3. Корпоративний - набирається номер визначається даними конфігурації корпоративного плану набору (Custom Bailing Plan).

Формат номера внутрішнього плану має такий вигляд:

• Фіксований: внутрішній національний код (якщо є) + код міста + номер абонента;

• Змінний: набирається номер заздрості від наступних факторів:

- локальний виклик (код міста відповідає коду, визначеного для шлюзу Інтернет-телефонії) - набирається тільки номер абонента;

- міжміський дзвінок (код міста відрізняється від коду, визначеного для шлюзу) - набирається внутрішній національний код (якщо є) + код міста + номер абонента;

• Корпоративний: набирається номер конфигурируется адміністратором і залежить від певних їм кодів.

Формат номера міжнародного плану має такий вигляд:

• Фіксований: код виходу на міжнародну мережу + код країни + код міста + номер абонента;

• Корпоративний: набирається номер конфігурується адміністратором і залежить від певних їм префіксів.

Формат номера приватного плану має такий вигляд:

• Фіксований: номер абонента;

• Змінний: набирається номер залежить від наступних факторів:

- локальний виклик (код приватної зони відповідає коду, визначеного для шлюзу) - набирається толь до номер абонента;

- міжміський дзвінок (код приватної зони відрізняється від коду, визначеного для шлюзу) - внутрішній національний код (якщо є) + код міста + номер абонента.

• Корпоративний: набирається номер конфигурируется адміністратором і залежить від певних їм кодів.

6. ОБЛАДНАННЯ IP-ТЕЛЕФОНІЇ

6.1. Класифікація обладнання IP-телефонії

На сьогоднішній день IP-телефонія – один із найбільш динамічних ринків у світі телекомунікацій. І оператори зв'язку, і виробники мережного обладнання, і учасники ринку комп'ютерної телефонії – всі намагаються запропонувати відмінні від інших рішення, що використовують різне обладнання.

В залежності від сфер застосування, кількості підтримуємих портів, набору реалізуємих послуг та інших факторів, все обладнання IP-телефонії можна віднести до наступних основних класів.

1) Апаратно-програмні комплексні платформи IP-телефонії.
2) Виділені або поєднані з іншим обладнанням шлюзи IP-телефонії.
3) УАТС з функціями IP-телефонії.
4) IP-телефони (апаратні та програмні).
5) Обладнання для відеоконференцій.

На сьогоднішній день *шлюзи* IP-телефонії, які призначені для перетворення оцифрованих голосових сигналів в IP-пакети для передавання їх по IP-мережам, є ключовими компонентами сьогоднішніх реалізацій IP-телефонії.

В цілому можна виділити декілька основних підходів для використання даного обладнання при реалізації мережі IP-телефонії, переваги та недоліки яких залежать від того, хто використовує дане обладнання і для яких користувачів.

Наприклад, якщо мережа IP-телефонії організовується великим регіональним оператором зв'язку, то кращими є рішення на виділених або інтегрованих в АТС шлюзах.

З іншого боку, провайдерам послуг Інтернет (ISP) при впровадженні послуг IP-телефонії найбільш доцільно використовувати рішення, основане на дооблаштуванні серверів доступу до мережі Інтернет функціями голосового перетворення. А для забезпечення заданої якості для голосового трафіку у маршрутизатори додаються функції QoS.

Якщо послуги IP-телефонії впроваджують великі фірми, то для них можна рекомендувати різні варіанти: дооблаштувати УАТС, яка є в наявності, функціями IP-телефонії або дооблаштувати корпоративний маршрутизатор, який є в наявності, голосовими портами, або встановити у локальній обчислювальній мережі апаратні або програмні IP-телефони.

З т.з. виробників вигідніше розвивати ті напрямки виробництва обладнання, якими вони давно займаються і по яким мають велику базу клієнтів. Наприклад, фірма Cisco – лідер з виробництва обладнання мереж передавання даних,

пропонує рішення на базі спеціалізованого обладнання IP-мереж. Інші фірми також прагнуть зайняти своє місце на ринку і орієнтуються в основному на *виділені шлюзи*, *голосові плати* або *абонентське обладнання*.

6.2 Апаратно-програмні комплекси платформи IP-телефонії

Комплексні рішення VoIP на ринку обладнання IP-телефонії – єдиний комплект апаратних і програмних засобів, які налаштовані на сумісну роботу. Таке рішення включає до свого складу:

- шлюз;
- gatekeeper;
- систему управління

та інші компоненти і призначене для використання у мережах великих операторів IP-телефонії.

Такими рішеннями є наступні комплекси:

1) Програмно-апаратний комплекс MultiVoice, який включає шлюз MultiVoice Gateway, контролер шлюзів MultiVoice Access Manager, систему управління і моніторингу Navis компанії Lucent Technologies. MultiVoice дозволяє вести телефонну розмову із звичайних телефонних апаратів, які з'єднані через відкриту або приватну пакетну мережу, з використанням стандартного шлюзу VoIP. Основою платформи MultiVoice є комутатори доступу до глобальних мереж, а в якості диспетчера (контролера шлюзів) використовується ПЗ MultiVoice Access Manager (MVAN).

2) шлюзи, пакет ПЗ для білінгу, маршрутизації та адміністрування;

3) шлюз/маршрутизатори серій 2600 та 3600, система управління Cisco Voice Manager;

4) шлюз, gatekeeper, менеджер, пакет ПЗ.

Рішення компанії Lucent Technologies

Апаратно-програмний комплекс Lucent Technologies Multi Voice для апаратури MAX включає в себе компоненти, які дозволяють постачальникам послуг і корпоративним клієнтам вводити голосові транспортні послуги реального часу на магістральних IP-мережах. Multi Voice дозволяє вести телефонну розмову із звичайних телефонних апаратів, які з'єднані через відкриту або приватну пакетну мережу, з використанням стандартного шлюзу VoIP.

Шлюз MultiVoice Gateway

Шлюз MultiVoice Gateway забезпечує сполучення ТМЗК та пакетної мережі IP. Для пакетної телефонної мережі він є точкою входу/виходу звичайних

телефонних дзвінків. Шлюз MultiVoice Gateway виконує наступні функції:

1) Кінцевий пристрій для стандартних мережних інтерфейсів ТМЗК (такі як T1, PRI, E1).

2) Підтримка різних голосових кодексів, що забезпечує різні рівні стискання голосу, зменшуючи вимоги до пропускної спроможності пакетної мережі.

3) Підтримка ехокомпенсації та виявлення пауз для підвищення якості голосу передавання мови та зменшення необхідної смуги пропускання.

4) Підтримка стеку протоколу ITU-T H.323 для розмови із звичайних телефонних апаратів по IP мережі;

5) Робота у парі з MultiVoice Access Manager для встановлення та роз'єднання викликів VoIP.

Схема комутатору доступу MAX 6000 приведена на рис.43. Цифровий сигнальний процесор управління (control DSP) взаємодіє з основним процесором шасі MAX (host CPU), який встановлено на материнській платі для зв'язку з мережею IP та виконання інших функцій управління. Після того, як голос оцифрований та стиснутий, він обробляється основним процесором для передавання по IP-мережі.

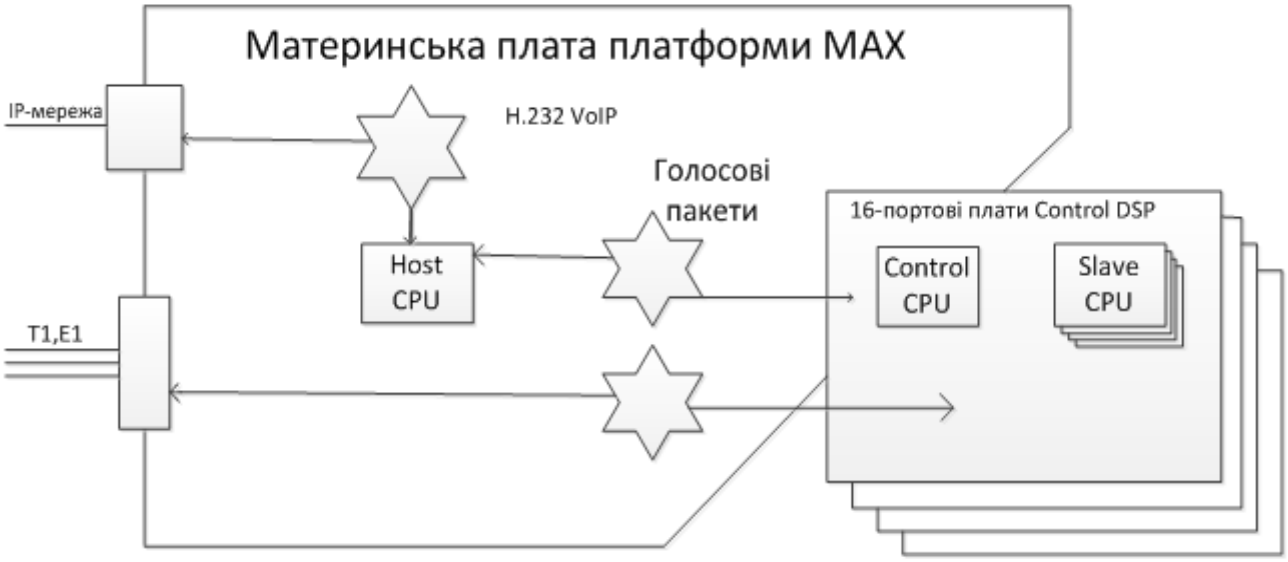

Рис.43. Схема комутатору доступу MAX 6000

*Менеджер доступу Multi Voice Access Manager (*gatekeeper*)*

Менеджер доступу Multi Voice Access Manager здійснює мережну маршрутизацію, з'єднуючи голосові виклики по IP мережі. Access Manager виконує наступні функції:

- Управління зоною H.323, що включає декілька шлюзів MultiVoice Gateway. Зоною вважаються декілька шлюзів H.323, що управляються визначеним менеджером Access Manager.
- Трансляція адрес стандартних національних та міжнародних телефонних номерів (номери E.164 і приватні плани нумерації) в IP адреси і у зворотньому напрямку.
- Підтримка аутентифікації користувачів та реєстрації шлюзів.
- Узгодження з додатками тарифікації.

На рис.44 показана типова схема мережі на базі обладнання Lucent Technologies для надавання послуг IP-телефонії.

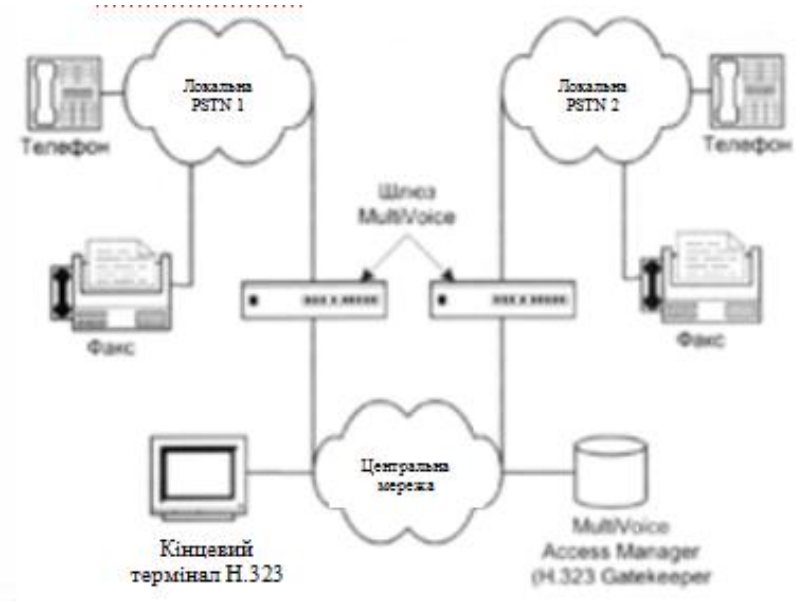

Рис.44. Схема мережі IP-телефонії на базі обладнання Lucent Technologies

Шлюз IP-телефонії VoIP з двома портами FXS та двома FXO (VIP-400)
VIP-400 (2xFXS+2xFXS/RJ-11 + 1x10/100Base-T

VIP-400 шлюз призначений для підключення двох аналогових телефонних ліній і двох цифрових для організації телефонного зв'язку через Інтернет.

• Два аналогових порти FXS дозволяють підключити телефонну станцію, телефон, факс.

• Два цифрових порти FXO дозволяють підключити цифрову телефонну станцію, цифровий телефон.

• Один порт FAST ETHERNET для підключення до глобальних мереж.

• Сумісний з аналогічним обладнанням CISCO, RAD.

• Управління через WEB/Telnet, консольний порт.

• **Проста установка** Один порт для ЛОМ і по два аналогових та цифрових порти під телефонну апаратуру.

• **Підтримка розповсюджених стандартів** G.729A/B, G.711, G.723.1. Це найбільш розповсюджені сервіси шлюзів IP-телефонії.
• **Проста мережна установка** Працює в мережах TCP/IP network. Має порт 10/ 100 Mbps.
• **Просте конфігурування** Вбудований Web браузер і підтримка Telnet або RS-232 консольний порт дозволяє просто налаштувати і управляти пристроями.
• **Швидкий набір** Підтримка програмованих функцій швидкого набору номера.
• **Підтримка стеку протокола H.323** H.323 дає можливість сумісності з переважною більшістю інтернет-додатків, включаючи Microsoft NetMeeting, NetSpeak, WebPhone і багато інших.

Рис.45. VIP-400

Рішення компанії Cisco Systems

Функції контролера шлюзу (gatekeeper) H.323 реалізуються в окремому додатковому маршрутизаторі (36xx або 26xx) з операційною системою IOS. Для кожного сімейства існує декілька різновидів операційної системи, вибір яких залежить від визначеного завдання.

Для моніторингу та управління мережею з підтримкою передавання мови Cisco пропонує Cisco Voice Manager. Voice Manager представляє собою додаток на Java і призначений для спрощення процесу розгортання та управління мережею з підтримкою передавання мови. Він полегшує конфігурацію голосових та факсимильних інтерфейсів та адміністрування плану голосового зв'язку, надає детальні сукупні та поточні звіти про виклики, вимірює такі параметри QoS, як затримка, втрата пакетів і тип послуги.

Коротко розглянемо продукти фірми Cisco, які найчастіше використовуються в мережах IP-телефонії.

Модульний маршрутизатор доступу Cisco 1750

Має потужний RISC процесор з тактовою частотою 48 МГц, підтримує від 16 до 48 Мбайт ОЗП і містить три слоти розширення для установки різних інтерфейс них карт. У слоти можна встановити голосові інтерфейсні карти VIC з двома портами FXO/FXS/E&M. На шасі є вбудований порт Ethernet 10/100, також є консольний порт. Використання Cisco 1750 разом з можливостями ОС IOS

дозволяє отримати VoIP H.323 v2 шлюз з 6-ма голосовими портами. Такий IP-шлюз, крім свого основного призначення, має багато функцій, які притаманні маршрутизатору, наприклад, встановлення черг для голосу та даних, підтримка шифрування інформації на швидкостях від 512 кбіт/с, можливість організації мережних екранів.

Модульні маршрутизатори серії Cisco 26xx

Побудовані на базі центральних процесорів. Містять на своєму шасі три слоти для встановлення різних модулів розширення. Всередині маршрутизатору є роз'єм для встановлення додаткового модуля розширення AIM, який зменшує завантаження основного процесору та покращує загальну продуктивність системи. На шасі маршрутизаторів серії 26xx є в наявності від одного до двух вбудованих портів Ethernet-Fast Ethernet, консольні порти управління. При побудові на базі сімейства 26xx голосового шлюзу з цифровими інтерфейсами телефонної мережі E1, в залежності від версії IOS, наявності модулю AIM, обсягу оперативної пам'яті та вибраного типу складності кодексів, можлива підтримка від 30 до 60 голосових портів.

Голосовий шлюз Cisco VG200

Представляє собою спрощену версію маршрутизатора сімейства 26xx. Виключені два слоти для встановлення інтерфейс них карт WIC, а також внутрішній слот розширення для модуля AIM. Оперативна пам'ять центрального процесора розширяється до 32 Мбайт. Підтримує до чотирьох інтерфейсів FXO/FXS/E&M або до двух цифрових трактів T1/-CAS, T1/E1 PRI та E1 CAS. На шасі вбудований інтерфейс ний порт Ethernet 10/100 Base-T.

Маршрутизатори Cisco 36xx для IP-телефонії

Найпопулярніше рішення у світі для передавання даних та Інтернет. Мають потужний процесор RISC та слотами розширення. Модульний принцип побудови маршрутизаторів Cisco Systemsдозволяє використовувати одні й ті самі уніфіковані модулі у різних платформах. Тому мережні модулі NM-HDV-1E1-30E (або NM-HDV-2E1-60) разом з інтерфейсними картами T1/E1 Multiflex Voice/WAN Interface Card (Multiflex VWIC) можна встановити і в 36 серію. Для того, щоб перетворити 3620 або 3640 у шлюз VoIP, необхідно придбати та встановити в один із слотів додатково модуль NM-1E з одним портом Ethernet 10Base-T. Таким чином, можна отримати ряд IP-шлюзів H.323 v2 наступної ємності:

- Cisco 3620 з одним модулем NM-HDV-2E1-60E, в залежності від вибраного типу складності кодексів – від 30 до 60 голосових портів;

- Cisco 3640 з трьома модулями NM-HDV-2E1-60E, в залежності від вибраного типу кодексів – від 90 до 180 голосових портів;
- Cisco 3660 містить на шасі вбудований порт Ethernet і завдяки цьому має можливість встановити шість модулів NM-HDV-2E1-60E, що в залежності від вибраного типу кодексів, дозволяє отримати від 180 до 360 голосових портів.

Сервер доступу Cisco AS5300

Побудований на основі процесору R4700 з тактовою частотою 150 МГц і був розроблений як гнучке та функціональне рішення для компаній провайдерів послуг Інтернет. Головна відмінність AS5300 від сімейств 26xx-36xx – вузькоспеціалізована концепція модульної архітектури. Шасі сервера доступу має три установочних слоти. Модулі розширення для серії AS5300 об'єднані у набори (наприклад, інтерфейсна карта на 4 тракти E1 PRI + карта на 60 цифрових модемів – рішення для організації сервера доступу в Інтернет по комутованим лініям). Інтерфейсні карти, в залежності від різновиду, дозволяють підключити від 4 до 8 цифрових трактів T1/E1 і до 4 портів WAN.

AS5300 містить інтерфейсну карту на 4 тракти E1 і карту постобробки з DSP на 60 голосових портів. Карта постобробки містить на собі ОЗП і окремий процесор з тактовою частотою 100 МГц, а також місця для плат DSP. Одна голосова карта подвійної щільності може забезпечити передавання до 60 одночасних розмов/факсів. Плата дозволяє дискретно нарощувати кількість голосових каналів шляхом встановлення невеликих плат – модулів DSP.

Кількість голосових портів не залежить від видів вибраних кодеків, а визначається лише пропускною спроможністю WAN-каналів.

Варіант використання серверу доступу Cisco AS5300 у мережі IP-телефонії показаний на рис.46.

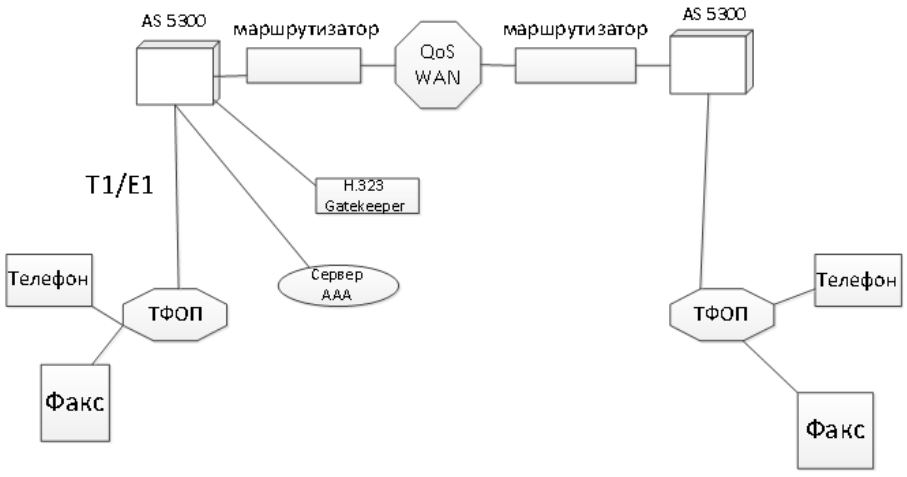

Рис.46. Побудова мережі IP-телефонії на базі Cisco AS5300

6.3 Обладнання шлюзів IP-телефонії

Маршрутизатор, комутатор доступу, шлюз можуть бути в одному виконанні. Допускає підключення близько 28 мовних каналів. Підтримує інтерфейси FXS, FXO, E&M, а також E1, PRI. Підтримує стандарт H.323, алгоритми кодування голосу G.711, G723.1 та G.729a. При цьому досягається компресія голосу до 5,3 кбіт/с. Маршрутизатори при необхідності облаштовуються функціями VoIP.

У деяких шлюзів обробка пакетів здійснюється потужним 64-розрядним процесором комп'ютера, а маршрутизація – вбудованими засобами SPARC. Один DSP обслуговує одну розмову (два канали). Кожний процесор цифрової обробки сигналів можна порівняти з RISC-процесором.

Є шлюзи, які представляють собою систему на базі Windows NT для організації моста між телефонною мережею та Інтернет з підтримкою дзвінків з телефону на телефон, з факсу на факс, з ПК на телефон, з телефону на ПК і з браузера Web на телефон. Користуватися системою дуже просто – після з'єднання із шлюзом автоматичний секретар запитує у викликаючого абонента телефонний номер адресата. Викликаючий абонент вводить телефонний номер з клавіатури звичайним чином. Місцевий шлюз автоматично визначає, що виклик повинен бути переадресований віддаленому шлюзу. Серед інших сервісів користувача - система інтерактивної голосової відповіді, відправлення факсів у реальному часі або з проміжним зберіганням в залежності від того, яку мету ставить перед собою користувач.

Існує ***голосовий шлюз-маршрутизатор***, який об'єднує функції мовного перетворення, маршрутизатора та контролера зони (gatekeeper) H.323. Завдяки підтримці великої кількості протоколів кодування мови VoIP-маршрутизатор може взаємодіяти з будь-якими голосовими шлюзами різних виробників. Такий шлюз-маршрутизатор забезпечує кодування мовного сигналу згідно рекомендацій G.711, G.723.1, G.723.1a, G.728, G.729, G.729a, G.729b, G.729ab. Модель має розвинені механізми забезпечення QoS, що є важливим для вирішення задач з передавання голосу через пакетні мережі. Найбільш важливі з них: фрагментація пакетів, ущільнення заголовків, управління смугою пропускання по протоколу RSVP, подавлення пауз. Додатково реалізовані механізми підвищення якості мови при відновленні: подавлення луно-сигналів, динамічна та статична буферизація коливань затримок сигналів, генерування комфортного шуму. Такий маршрутизатор підтримує інтерфейси FXS, FXO, E&M, а також E1, BRI, PRI. Може обробляти до 30 голосових каналів. Має один мережний інтерфейс 10Base-T. Підтримує сигналізацію по виділеному (CAS) та загальному (CCS) каналу для УАТС, може об'єднувати офісні станції.

Голосовий шлюз-маршрутизатор корпорації NEC

Голосовий шлюз-маршрутизатор IP45/951 японської корпорації NEC об'єднує функції мовного перетворення, маршрутизатора і контролера зони (gatekeeper) H.323. У подальшому планується включити функції серверів аутентифікації і білінгу.

Завдяки підтримці великої кількості протоколів кодування мови VoIP-маршрутизатор може взаємодіяти з будь-якими голосовими шлюзами різних виробників. За даними корпорації NEC, їх шлюз-маршрутизатор забезпечує кодування мовного сигналу відповідно до рекомендацій G.711, G.723.1, G.723.1a, G.728, G.729a, G.729b, G.729ab.

Модель володіє розвиненими механізмами забезпечення QoS, що важливо для вирішення завдань по передаванню голоса через пакетні мережі. Найбільш важливі з них: фрагментація пакетів, ущільнення заголовків, управління смугою пропускання по протоколу RSVP, подавлення пауз. Додатково реалізовані механізми підвищення якості мови та відновленні: подавлення ехо-сигналів, динамічна і статична буферизація коливань затримок сигналів, генерація комфортного шуму.

Маршрутизатор IP45/951 підтримує наступні голосові інтерфейси: для аналогових каналів – E&M та FXS, скоро буде підтримуватися FXO; для цифрових каналів - E1/T1, планується включити інтерфейси ISDN BRI та PRI. Цейпристрій може обробляти до 30 мовних каналів. Мережний інтерфейс тільки один – 10BaseT.

Для ілюстрації можливостей IP45/951 на рис.47 представлений типовий варіант побудови фрагменту корпоративної мережі, яка з'єднує центральний офіс, філіал і невелику торгову точку (наприклад, пункт обміну валюти). Для організації каналів зв'язку між ними можна використовувати мережі протоколів Frame Relay або IP. Після появи інтерфейсів ISDN для цієї мети цілком підійдуть BRI або PRI.

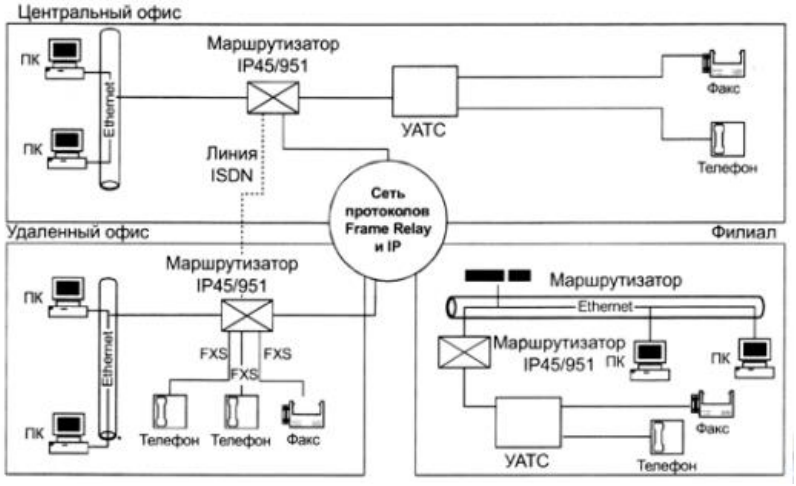

Рис.47. Фрагмент типової корпоративної мережі на базі шлюзу-маршрутизатора IP45/951 корпорації NEC

Оскільки маршрутизатор підтримує сигналізацію по виділеному (CAS) та загальному (CCS) каналу для УАТС, він може об'єднувати офісні станції. Таке рішення дозволяє зменшити необхідну кількість голосових портів і плавно інтегруватися в існуючу інфраструктуру.

Business Communications Manager фірми Nortel Networks

Універсальна система Business Communications Manager (BCM) фірми Nortel Networks одночасно виконує функції офісної АТС і шлюзу IP-телефонії, маршрутизатора і пристрою доступу у територіально розподілену мережу (WAN). У ній реалізовані різноманітні IP-сервіси: потужний ез проводов екран забезпечує безпечну роботу в Інтернет, кешування DNS-імен та вмісту Web- сторінок прискорює цю роботу, а DHCP-сервер полегшує адміністрування мережі. Вбудований сервер Windows NT дозволяє використовувати широкий набір прикладного програмного забезпечення, оптимізованого для роботи на цій операційній платформі.

При передаванні пакетних даних у системі реалізуються такі функції:

• маршрутизатор IP/IPX (статичний, RIP, OSPF) з підтримкою DiffServ;
• протоколи WAN (Frame Relay, PPP, MLPP);
• резервування основного WAN-каналу по комутованому (V.90 або ISDN BRI/ PRI);
• динамічне конфігурування (сервер DHCP);
• кешування або DNS і вмісту Web-сторінок;
• трансляція адрес (NAT).

Система BCM дозволяє реалізувати такі мовні та інтегровані додатки:

• IP – телефонія;
• мовна пошта і автосекретар;
• уніфікована обробка повідомлень;
• центр обслуговування викликів;
• консоль телефоністки на базі ПК;
• комп'ютерно-телефонна інтеграція (CTI);
• безпроводовий мікростільниковий зв'язок Companion (DECT з версії 2.5).

На базі системи BCM можливе повне (телефонія + Інтернет) комунікаційне оснащення невеликого і середнього офісу (рис.48). Ємність системи версії 2.0 становить 80 телефонних абонентів, у версії 2.5/3 вона збільшена до 180 абонентів. Можливе підключення до системи апаратних і програмних IP-телефонів Nortel Networks. Більш того, версія 2.5 дозволяє використовувати з BCM ез проводові H.323-термінали.

Рис.48. Реалізація мережі IP-телефонії на базі системи BCM фірми Nortel Networks

6.4 УАТС з функціями IP-телефонії

Теперішні УАТС виконують роль комунікаційного серверів, які підключені до ЛОМ і виконують транзакції в режимі реального часу практично із 100%-ою надійністю. В останніх версіях УАТС реалізована підтримка послуг IP-телефонії, а самі вони стали повноцінними вузлами IP-мереж.

IP-шлюз може бути встановленою платою в УАТС або окремим пристроєм.

При інтеграції IP-телефонії безпосередньо в УАТС абонент отримує доступ до більш широкого набору сервісів.

Забезпечуючи зв'язок віддалених УАТС через IP-мережу, шлюзи передають і телефонну сигналізацію. Стосовно сервісу, IP-УАТС нічим не відрізняється від класичних, просто мова і сигналізація передаються по IP-мережі (рис.49).

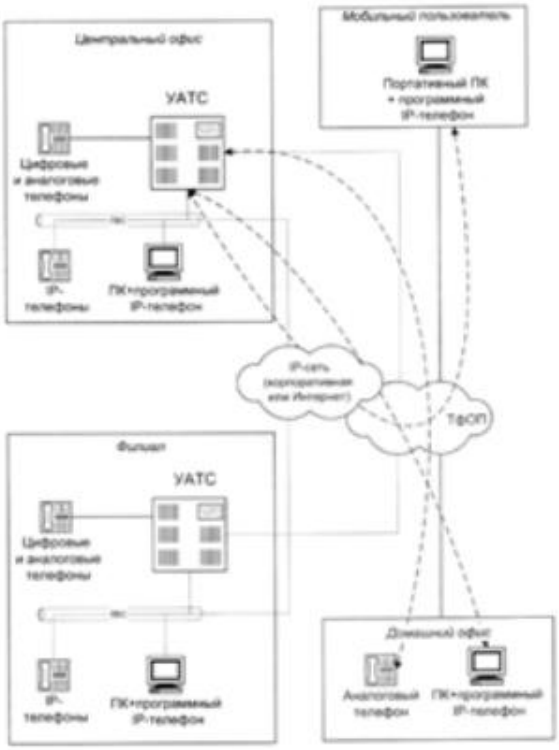

Рис.49. Реалізація корпоративної мережі IP-телефонії

Шлюзи, які використовуються в УАТС, постійно відслідковують якість зв'язку і, якщо вона стає нижче заданого рівня, переводять з'єднання у традиційні мережі (рис.50).

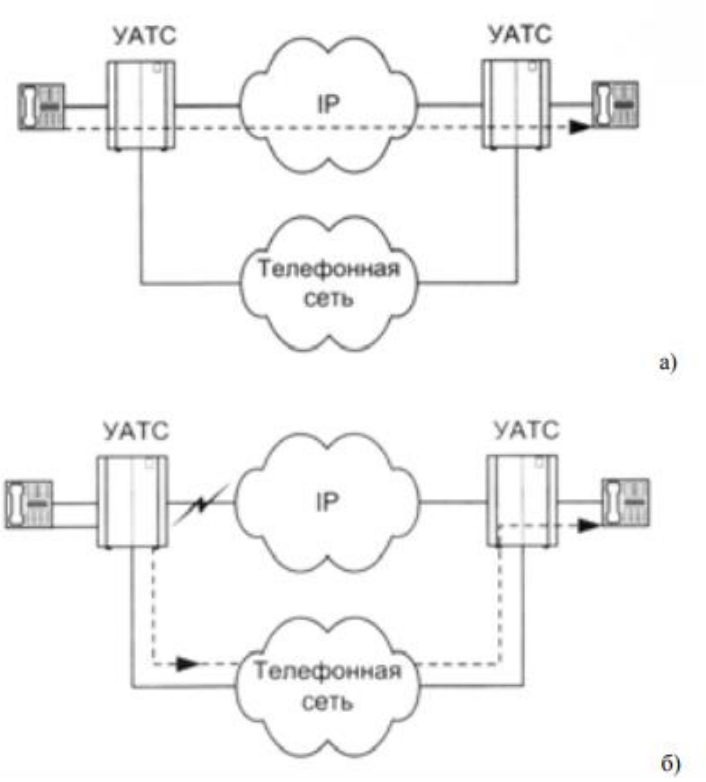

Рис.50. Перехід IP-УАТС на телефонну мережу при різкому погіршенні якості IP-мережі

Більшість IP-шлюзів виконані у вигляді плат/модулів, що встановлюються у стативи УАТС. Стосовно алгоритмів кодування, найбільш популярними є звичайна ІКМ (G.711), а також механізми G.723 (5,3/6,3 кбіт/с) та G.729 (8 кбіт/с), забезпечуючи суттєве стискання сигналу. Всі виробники забезпечили відповідність своїх шлюзів рекомендації Н.323.

Провідні виробники IP-УАТС випускають апаратні та програмні IP-телефони. Апаратні IP-телефони підключаються безпосередньо до локальної мережі по інтерфейсу Ethernet і по зовнішньому вигляду та функціональності є практично повними аналогами традиційних апаратів, що виробляються цими ж компаніями. Такі апарати мають різні функціональні можливості.

Програмні телефони реалізовані у вигляді прикладних програм, а їх функціонування повністю залежить від роботи ПК. Таке рішення IP-телефону дозволяє використовувати різні додатки комп'ютерно-телефонної інтеграції, наприклад, телефонну книгу, програму-менеджер управління викликами, графічний інтерфейс для роботи з голосовою поштою.

УАТС OmniPCX 4400 компанії Alcatel

УАТС OmniPCX 4400 має вбудовану підтримку IP. Архітектура станції така, що її ядро складає UNIX-сервер, а шина - повнозв'язна коміркова структура ATM (звідси торгова марка технології - «кристал»). Така платформа - цілком придатна для IP оточення.

Alcatel має у своєму розпорядженні ПЗ для організації на базі мультимедійного комп'ютера робочого місця Alcatel 4980. Воно інтегрується в існуючі платформи колективної роботи і забезпечує повний доступ до всіх сервісів OmniPCX. Крім того, компанія пропонує ПЗ для адміністрування телефонних сервісів.

OmniPCX 4400 підтримує таку важливу функцію, як гарантований мінімум якості розмов і їх безперервність. Якщо, крім IP-з'єднання, станція має традиційне (як резерв або паралельну альтернативу), то при погіршенні якості зв'язку через IP вона переключиться на нього. Оцінка якості з'єднання на основі параметрів проходження пакетів здійснюється безперервно, і якщо на станцію надходить виклик, а параметри IP-з'єднання нижче допустимих, то станція задіює традиційні канали. Крім того, перемикання на резервну лінію може здійснюватися динамічно, для чого OmniPCX повинні бути встановлені по обидві сторони з’єднання. Динамічне перемикання відбувається прозоро для абонента (за виключенням зміни звуку), без переривання розмови.

6.5. IP-телефони

Апаратний IP-телефон – самостійний пристрій, який не вимагає підключення до телефонної лінії і дозволяє користуватися послугами IP-мережі для здійснення міжміських і міжнродних переговорів, наприклад, через Інтернет-канали.

IP-телефону присвоюється власний телефонний номер, на який може подзвонити будь-який абонент IP-мережі. На відміну від звичного варіанту доступу до послуг, коли абонент повинен спочатку подзвонити по міському телефону доступу до провайдера IP-мережі, набрати свій PIN-код і тільки після цього набрати необхідний телефонний номер, IP-телефон використовується як класичний телефон. Абонент просто знімає трубку і набирає необхідний номер. IP-телефон призначений як для приватного використання, так і для встановлення в офісах. В останньому випадку, при використанні декількох апаратів, з’являється можливість організувати офісний або корпоративний зв`язок без використання класичної телефонії. При цьому абсолютно неважливе територіальне розміщення апаратів – організація зв`язку буде однаково простою як і у випадку, якщо вони розміщені на сусідніх столах, так і при установці їх у протилежних точках земної кулі. Для підключення IP-телефону необхідно тільки наявність підключення до IP-мережі (у випадку мережі Інтернет – бажано постійно діючого).

Структурна схема IP-телефону показана на рис.51.

IP-телефон включає в себе наступні компоненти:

- інтерфейс користувача (User Interface);
- мовний інтерфейс (Voice Interface);
- мережний інтерфейс (Network Interface);
- блок процесору (Processor Core);
- зв`язна логіка (associated logic).

Інтерфейс користувача забезпечує реалізацію традиційних функцій телефону. Як мінімум, це клавіатури для набору номера (кнопки 0-9, *, #) і звуковий індикатор для сигналізації про вхідні виклики користувачу. На більш складних телефонних апаратах використовуються додаткові клавіші, які забезпечують повторний набір номеру, зберігання номерів, переадресацію, конференцзв`язок і т.д. Звичайно використовується дисплей для відображення підказки користувачеві, номеру, що набирається, інформації про вхідні виклики і т.д. У деяких моделях телефон обладнаний послідовним інтерфейсом для підключення пристроїв типу PDA (персональний цифровий помічник), що дозволяє забезпечувати синхронізацію телефонної інформації, полегшує автоматичний набір номеру і т.д.

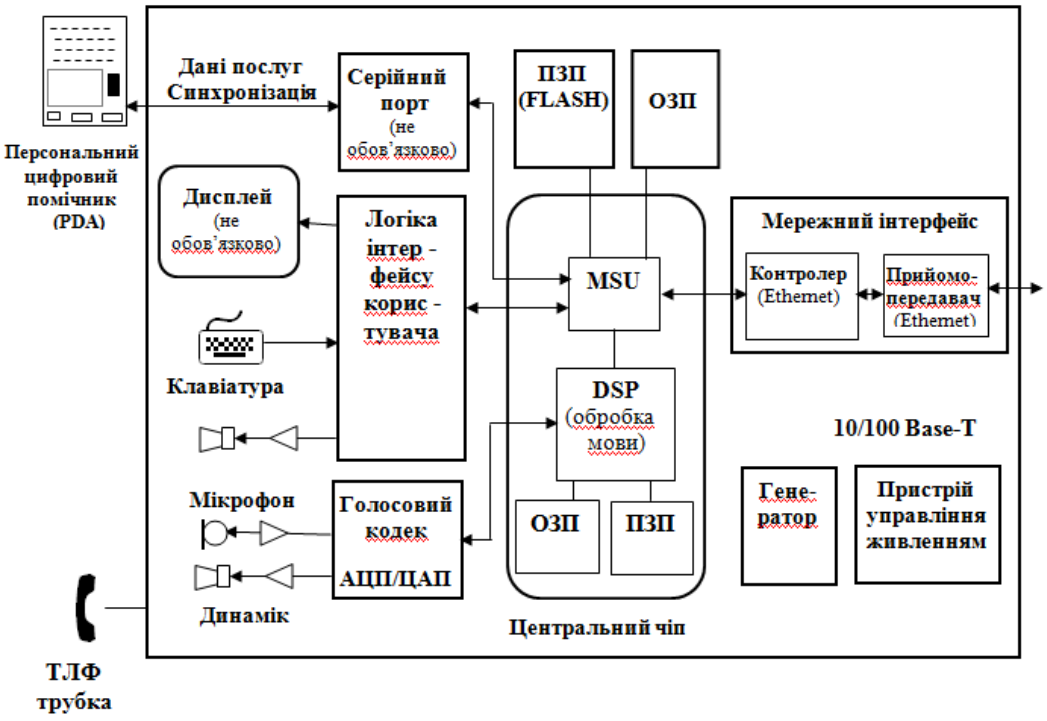

Рис.51. Структурна схема IP-телефону

Мовний інтерфейс забезпечує перетворення аналогового голосового сигналу у цифрові відліки. Мовні сигнали від мікрофону дискретизуються з частотою 8 кГц, що створює після кодера з імпульсно-кодовою модуляцією цифровий потік даних на процесор із швидкістю 64 кбіт/с. Зворотній процес дозволяє перетворити потік даних 64 кбіт/с через декодер ІКМ в аналогової мовний сигнал, який передається

у телефонній капсуль або гучномовець.

Мережний інтерфейс забезпечує передавання і прийом мовних пакетів від/у телефону у локальну обчислювальну мережу найчастіше з інтерфейсом 10BaseT або 100BaseT Ethernet, що працює по протоколу TCP/IP. IP-телефон може мати другий роз'єм RJ - 45 Ethernet для підключення персонального комп'ютеру, щоб спільно використовувати одне підключення до настінної розетки.

Блок процесора виконує обробку голосової інформації, обробку сигналізації, обробку протоколу і функції програмного управління всією схемою телефону. Як показано на рис.51, він складається з цифрового сигнального процесору (DSP) для виконання функцій обробки голосу і пристрою мікроконтролеру (MCU) для виконання інших функцій управління. Для забезпечення гарантованого зберігання програмного забезпечення у телефоні використовується флеш-пам'ять.

Налаштування IP-телефону дуже просте і може виконуватися самим абонентом відповідно до інструкції. Абоненту видаються авторизаційні дані (ім'я, PIN - код) і виділяється унікальний телефонний номер для дзвінків з іншого IP-телефону.

Переваги використання апаратних IP-телефонів:

• простота і економія технічних ресурсів при організації корпоративної або приватної мережі зв'язку, оскільки не використовується класична телефонія;

• прискорення процесу дозвону - виключаються дзвінок на телефон доступу до мережі IP-телефонії і набір PIN-коду;

• мобільність - IP-телефон може бути швидко переміщений у будь-яку іншу точку з мінімальним переналаштуванням або взагалі без нього;

• можливість прямих дзвінків на інший IP-телефон;

• для операторів - економія технічних ресурсів, так як не використовуються лінії зв'язку.

Приклад зв'язку за допомогою IP-телефону через мережу Інтернет показаний на рис.10. Тут в якості управляючого протоколу використовується протокол SIP (Session Initiation Protocol). Функції авторизації і обліку, а також забезпечення взаємодії з компонентами IP-мережі, що працюють на основі протоколу H.323, виконують SIP-Proxy і SIP-H.323 Signalling Gateway.

Дзвінки враховуються так само, як і дзвінки через шлюз оператора мережі IP-телефону. Для клієнтів, які використовують IP-телефон, оператор може створити спеціальний тарифний план. Біллінгова система виконує спеціальну перевірку для клієнтів з таким тарифним планом і не допускає дзвінків звичайним шляхом, через вхідні телефони загальнодоступного шлюзу.

В якості недоліків використання IP-телефонів потрібно зазначити необхідність локального живлення, а це додаткові незручності і зниження надійності. Без дистанційного живлення IP-телефони не отримають широкомасштабного розповсюдження.

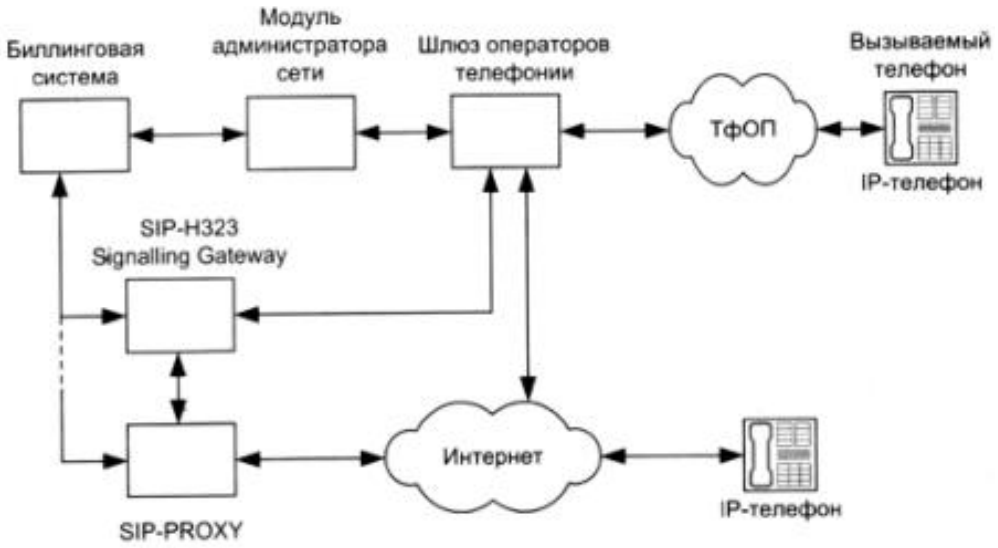

Рис.52. Схема зв’язку через Інтернет з використанням IP-телефону

Слід зазначити, що крім апаратної існують і програмні реалізації IP-телефонів. У цьому випадку персональний комп'ютер, який облаштований телефонною гарнітурою або мікрофоном і колонками, перетворюється у багатофункціональний комунікаційний центр. Користувач персонального комп'ютера, крім доступу до звичайного телефонного сервісу, отримує масу інших можливостей, які підвищують продуктивність його роботи. Так, завдяки наявності стандартного телефонного прикладного програмного інтерфейсу TAPI до інших програм, можна автоматично отримувати інформацію про абонента, який телефонує (витягується з бази даних за його ідентифікатором), а також використовувати зручні інтерфейси для контролю за телефонними викликами та роботи з голосовою поштою.

Далі розглянуті найбільш відомі апаратні IP-телефони, що випускаються провідними світовими виробниками телекомунікаційного обладнання.

IP-телефони фірми Cisco

Фірма Cisco одна з перших почала випускати IP-телефони. Настільний IP-телефон існує у варіантах: IP Ethernet-телефон серії Cisco IP-Phone, який підключається безпосередньо у роз’єм Ethernet RJ-45 (відрізняється від традиційного телефонного роз'єму RJ-11) і телефонна трубка/телефон-навушники, які підключаються безпосередньо до персонального комп'ютера. Другий варіант сподобається тим користувачам, які інтенсивно використовують телефон разом з ПК.

IP Ethernet-телефон - це новий пристрій, який схожий на звичайний телефон, що підключається до УАТС, але, на відміну від нього, приєднується до Ethernet-

порту комутатора. IP-телефон забезпечує якість звуку, що порівнюється із звичайним телефоном, а також має програмований прискорений набір номеру та інші розширені функції. У IP-телефона багато спільного з ПК. Він може працювати, як звичайне IP-пристрій, і мати мати власну IP-адресу. Оскільки IP-телефон повністю сумісний із стандартом H.323, з його допомогою можна зв'язатися з будь-яким іншим H.323-сумісний з пристроєм або ПЗ, наприклад, з Microsoft NetMeeting. Нижче наведені деякі основні характеристики IP- телефону:

• 10 BaseT Ethernet (RJ-45);

• програмовані кнопки для функцій, прискореного набору та індикатор стану ліній;

• IP-адреса і передавання сигналізації (по TCP/IP) через CallManager;

• підтримка стандарту H.323;

• вбудована аудіокомпресія: G.711, G.7234;

• призначення IP-адреси та конфігурація через сервіси DHCP, BootP або з клавіатури;

• адміністрування або налаштування функціональних кнопок через Web-браузер;

• вбудоване шифрування голосового трафіку для захисту від прослуховування;

• третя пара проводів для резервування живлення в разі відмов електропостачання;

• взаємодія ПК і додатку NetMeeting за допомогою єдиної кнопки (T.120); для підтримки таких функцій, як спільне використання додатків, відео, chat та whiteboarding;

• вбудований порт мережного концентратора для каскадного підключення пристроїв Ethernet-телефонів і ПК (реалізовано лише у моделі 12);

• різноманітні моделі: спікерфон, дисплей, багатокнопочні апарати - Cisco поставляє 12 і 30 кнопочні моделі IP-телефонів.

До складу серії Cisco IP-Phone входять чотири моделі, характеристики яких наведені у табл.6.

Табл.6. Характеристики IP - телефонів серії Cisco IP-Phone

Тип IP-телефону	**7910**	**7910+SW**	**7940**	**7960**
Кількість програмованих клавіш	4	4	6	10
Тип дисплею	48-символьний ЖК-дисплей	48-символьний ЖК-дисплей	Великий ЖК-дисплей	Великий ЖК-дисплей

Підключення до мережі Ethernet	Пряме підключення	Пряме підключення	Вбудований Hub, 2 порта Ethernet 10/100 Base-Tx Ethernet (RJ-45)	Пряме підключення
Кількість та тип портів	1 порт 10BaseT (RJ-45)	2 порти 10/100BaseT	1 порт EIA/TIA RS-232	2 порти 10/100Base-Tx Ethernet (RJ-45), 1 порт EIA/TIA RS-232
Компресія	G.711, G.729a	G.711, G.729a	G.711, G.729a	G.711, G.729a

На РК-дисплей усіх моделей Cisco IP Telephone виводяться дата і час, номер і ім'я викликаючого абонента, цифри набираємого номеру. Крім того, в моделях 7940 і 7960 визначається і висвічується тип виклику: внутрішній або зовнішній.

Також існує чисто програмна версія телефону для ПК. Програмний продукт Cisco IP SoftPhone дозволяє емулювати IP-телефон на комп'ютерах. ПЗ віртуального телефону може бути встановленим на ПК або мобільний комп'ютер, оснащений звуковою картою та мікрофоном. Подібно IP-телефону Cisco, що має вбудований програмний інтерфейс Microsoft NetMeeting API, викликаюча сторона може встановлювати сесії NetMeeting натисканням єдиної функціональної кнопки і використовувати додатки для відео та функції whiteboarding. Cisco IP SoftPhone повністю сумісний з телефоном Cisco IP і підтримує компресії G.711, G.723.1, G.729A.

IP-телефони компанії Alcatel

До складу серії IP-телефонів компанії Alcatel входять моделі телефонів: Premium IP і Advanced IP. Обидві моделі телефонів можуть підключатися до декількох ліній, мають гучномовний зв'язок, набір без зняття трубки і набір по імені за допомогою вбудованої буквено-цифровий клавіатури. Але перша модель Premium IP має менше програмованих клавіш, дисплей меншого розміру і орієнтована на індивідуальне використання. Друга модель Advanced IP призначена для групового використання і забезпечує видавання на дисплей одночасно декількох рядків, контроль зв’язку та фільтрацію дзвінків. Характеристики IP-телефонів серії Reflexes™ Models компанії Alcatel приведені у табл.7.

Табл.7. Характеристики IP-телефонів серії Reflexes™ Models компанії Alcatel

Характеристики телефонів	**Premium IP**	**Advanced IP**
Кількість програмованих клавіш	12	24
Навантаження, що обслуговується	Орієнтований на індивіду-альне використання	Орієнтований на групове використання
Розміри дисплею (рядків х символів)	1х20	2х40 (з навігатором)
Наявність гучномовця	Так	Так
Набір без зняття трубки	Так	Так
Набір по імені	Так (вбудована буквенно-цифрова клавіатура)	Так (вбудована буквенно-цифрова клавіатура)
Наявність інтерфейсу до Advanced Communication	Так (інтегрований)	Так (інтегрований)

Відмінними рисами телефонів на основі протоколу SIP:

- вбудована підтримка Java; Java-інтерфейси прикладного програмування для телефонії;
- графічний інтерфейс доступу до функцій ПК, який вбудований у телефонний апарат;
- традиційні та принципово нові телефонні функції;
- підтримка функцій забезпечення безпеки та якості обслуговування, включаючи DiffServ та MPLS.

Виконання цих функцій забезпечує наступні переваги для користувачів:

- відкрите середовище розробки додатків;
- виклик абонента по його ідентифікатору URL, а також за допомогою додатків встановлення зв’язку;
- прискорений виклик абонента, інтуїтивно зрозумілий доступ до додатків;
- підтримка функцій вимикання телефону без відключення абонента (Hold), пересилання та ретрансляції викликів, ведення журналу телефонних перемов, організації конференцій та ін.;
- захист переговорів, які ведуться, від прослуховування і висока якість звуку.

6.6. Системи відеоконференцій і обладнання для них

Відеоконференцзв'язок (ВКЗ) надає можливість проводити наради з діловими партнерами, керівниками, співробітниками, створюючи «ефект присутності» і суттєво розширюючи можливості спілкування. Сучасні системи ВКЗ дозволяють легко обмінюватися із співрозмовниками будь-якою візуальною інформацією, графіками, слайдами і відео-роликами у реальному масштабі часу. Системи ВКЗ незамінні для організації нарад керівників, віддаленого навчання співробітників, проведення семінарів, конференцій і презентацій. Послуга ВКЗ розширює можливості спілкування.

Відеотелефони конференцзв'язку і станції відеоконференцій надають нові можливості використання мережних технологій – проведення відеоконференцій через Інтернет та локальні мережі з використанням протоколів IP-телефонії. Все, що необхідно – висока швидкість пропускання мережі для забезпечення якісного передавання зображення. Використовуючи прості процедури встановлення через допоміжну клавіатуру по телефону, ми можемо за декілька хвилин встановити і використати голосовий та відеоконференцзв'язок.

Відеотелефони конференцзв'язку і станції відеоконференцій сумісні з протоколом H.323, що позбавляє від необхідності використовувати спеціальні шлюзи і програмне забезпечення для встановлення та проведення сеансів зв'язку. Підтримка шлюзу (Gatekeeper) і MCU дозволяє зробити бізнес-контакти швидкими та ефективними.

Щодо застосування потрібно з'єднати відео пристрої конференцзв'язку з нашою локальною мережею Ethernet або модемом DSL і ми зможемо насолоджуватися високоякісним відеоконференцзв'язком. З PPPoE, DHCP та динамічною підтримкою DNS, статична IP-адреса не потрібна. Оскільки обладнання буде працювати в існуючій інфраструктурі (мережа, Інтернет), не потрібно ніяких додаткових витрат. Можна один з одним входити в контакт з нашими друзями, родичами, колегами та діловими партнерами у всьому світі з нашого офісу, зали засідань або навіть нашого будинку.

Основні характеристики обладнання відеоконференцзв'язку

- сумісність з ITU H.323 v.2;
- підтримка H.263 відео кодека та G.723.1, G.711 аудіо кодека;
- сумісність з H.323 VoIP шлюзом, Gatekeeper, MCU (Multipoint Control Unit) та Microsoft NetMeeting;
- вбудована високоякісна CCD камера;
- двостороннє одночасне передавання голосу;

- підтримка статичного IP, PPPoE, DHCP Connection;
- підтримка Dynamic DNS;
- підтримка швидкості передавання кадрів до 30 в секунду;
- телефонна книга на 100 номерів із швидким пошуком;
- функція передавання миттєвих знімків;
- постійний контроль інформації про якість мережного з'єднання;
- підтримка відео автовідповідача;
- вбудований мікрофон;
- вбудований гучномовець;
- 1 спарений RCA Audio/Video вихід для підключення телевізору.

Інтернет відео сервер оцифровує аналогове відео зображення і передає його з незмінною частотою кадрів через IP мережі, даючи можливість віддаленого відео перегляду у реальному часі по локальній мережі або Інтернету. Відео сервер облаштований вбудованим детектором руху потужними функціями моніторингу, які основані на тригерних або запланованих подіях. Облаштований захистом, таким як фільтр IP адрес та багаторівневий захист паролю.

6.7. Рішення для розгортання телефонної мережі

Asterisk

Asterisk - програмна АТС, здатна комутувати як VoIP виклики, так і виклики, які здійснюються між IP-телефонами і традиційної телефонною мережею загального користування.

Протоколи, які підтримуються: IAX, SIP, H.323, Skinny, UNIStim.

Кодеки, які підтримуються: G.711 (ulaw і alaw), G.722, G.723, G.729, GSM, iLBC, LPC-10, Speex.

Asterisk - відкрите програмне забезпечення, яке динамічно розвивається. Може бути встановлене без огляду на ліцензування. Це робить дану програмну АТС привабливою для малого і середнього бізнесу. Кількість абонентів в мережі може досягати 2000 і обмежене тільки потужністю серверу.

Ще одна перевага Asterisk - можливість гнучкого налаштування. Весь необхідний функціонал або вже реалізований, або може бути дописаний самостійно без істотних тимчасових і грошових витрат. Цьому сприяє принцип: одна задача - один програмний модуль.

У порівнянні з рішеннями від таких вендорів, як Cisco або Avaya, Asterisk привабливий ще й вартістю розгортання. Фактично всі витрати зводяться тільки до покупки телефонних апаратів і сервера, здатного забезпечити необхідне навантаження на мережу. Сама програма абсолютно безкоштовна.

Cisco Unified Communication Manager (CallManager)

CallManager призначений скоріше для великих мереж, що включають до 30000 абонентів. Даний програмно-апаратний комплекс забезпечує надійність роботи і дозволяє конфігурувати безліч параметрів, таких як переадресація дзвінків або голосове меню. Існує й "полегшена" express версія, яка призначена для невеликих офісів.

З переваг Cisco CallManager слід відзначити в першу чергу відому технічну підтримку корпорації Cisco. При відповідному рівні контракту на обслуговування, будь-яка проблема, починаючи з питань по налаштуванню і закінчуючи вийшовшим з ладу обладнанням, буде вирішена практично миттєво. Тому Cisco CallManager підійде компаніям, готовим платити чималі гроші, але й отримувати при цьому високу якість обслуговування.

Avaya IP Office

Система IP Office може стати непоганим вибором для середнього розміру телефонної мережі. Кількість абонентів тут обмежена не тільки потужністю серверу, але й кількістю придбаних ліцензій. Ліцензувати необхідно практично все - плати розширення, додатки, які використовуються, і т.д., що може доставити певні незручності.

Конфігурація може здійснюватися через ряд програм, але найбільш популярна і проста в обігу - Avaya IP Office Manager. Також можливе управління через консоль за допомогою Avaya Terminal Emulator.

В цілому, продукція корпорації Avaya не обмежується одним IP Office. Avaya, яка у 2009 році злилася ще з одним відомим виробником Nortel, є визнаним лідером на ринку обладнання для IP-телефонії.

7. МОБІЛЬНІСТЬ В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

7.1. різновиди мобільності

Мережі IP-телефонії повинні підтримувати такі чотири типи мобільності.

1. Мобільність користувача - здатність користувача з'єднуватися з мережею IP телефонії, використовуючи для з'єднання різні термінали і типи терміналів.

2. Мобільність терміналу - здатність терміналу міняти фізичне місцезнаходження, зберігаючи можливість з'єднання з мережею. У свою чергу мобільність терміналу підрозділяється на два види.

- Дискретна мобільність терміналу (roaming) - зміна фізичного місцезнаходження терміналу за межами сеансу зв'язку з мережею.

- Безперервна мобільність терміналу (handover) - зміна фізичного місцезнаходження терміналу в межах сеансу зв'язку з мережею з втратою або без втрати даних, що передаються.

3. Мобільність обслуговування - надає абоненту можливість скористатися послугою, на яку він підписався, незалежно від місцезнаходження і типу терміналу.

4. Режим віртуальної домашньої мережі - те ж саме, що і мобільність обслуговування, але стосується не однієї послуги, а пакета послуг. При цьому, в залежності від конкретної послуги, що надається абоненту, в його обслуговування може бути залучений тільки сервер домашньої мережі або необхідна взаємодія сервера домашньої мережі з сервером візитною мережі.

Підтримка того чи іншого типу мобільності залежить, перш за все, від протоколу, який застосовується в IP- мережі. Далі будуть розглянуті можливості мобільності в мережах IP-телефонії, що використовують протоколи IPv4, IPv6 і SIP, а також в мережах стандарту H.323.

Крім того, доступ до мереж IP-телефонії можуть отримати і абоненти стільникових мереж. Однією з перспективних технологій, що забезпечують доступ мобільного абонента стільникового зв'язку до мереж передачі даних, є система пакетний радіозв'язок загального користування (GPRS). Ця технологія спочатку розроблена для стандарту стільникового зв'язку GSM, проте вона вже адаптована для третього покоління стандартів стільникового зв'язку, наприклад UMTS.

7.2. Ідентифікація терміналу і користувача

Для реалізації послуг мобільності користувача і терміналу потрібно їх ідентифікація на різних рівнях. Термінал може бути ідентифікований як

обладнання або як телефонне додаток IP, яке може управляти різними елементами мережі.

Термінал має визначається одним із таких:

• ідентифікатор терміналу (транспортна адреса, ідентифікатор обладнання);

• ідентифікатор додатки (ідентифікатор кінцевої точки, точки доступу, адреси додатків транспортного рівня).

Повна адреса терміналу на транспортному рівні повинен містити IP адреса, тип транспортного протоколу, номер порту і тип прикладного протоколу.

Для визначення користувача використовуються визначається одним із таких:

• ідентифікатор користувача (рівень додатків);

• абонентський ідентифікатор (транспортний рівень);

• роумінговий ідентифікатор користувача (по суті абонентський ідентифікатор прикладного рівня, який може відрізнятися, або не відрізнятися від абонентського ідентифікатора транспортного рівня).

Роумінговий ідентифікатор використовується тільки один раз. Оператор формує безліч роумінгових ідентифікаторів, які застосовуються послідовно. Таким чином, щоб досягти необхідного абонента, в IP-телефонії використовуються адреси транспортного рівня і тимчасові ідентифікатори. До всіх ідентифікаторів пред'являються особливі вимоги з безпеки, і вони "не повинні передаватися у відкритому вигляді.

7.3. Сценарії мобільності в мережах IP-телефонії

Всі об'єкти, які беруть участь у процедурі мобільності, можна поділити на такі функціональні елементи.

• IP Application Point of Attachment (APoA) - точка підключення IP додатки. Це компонент, наприклад, gatekeeper, в якому термінал реєструється на прикладному рівні, наприклад, термінал H.323. У функції APoA входить забезпечення з'єднання мобільного абонента з мережею на прикладному рівні.

• Ноті Entity (HE) - домашній компонент, який управляє встановленням з'єднання з абонентом, зберігає дані про профіль абонента, надає APoA дані про поточне місцезнаходження абонента.

• Network Point of Attachment (NPoA) - точка підключення мережі. Це компонент, який забезпечує з'єднання між різними IP мережами. У його функції входить забезпечення зв'язку мобільного абонента з мережею на транспортному рівні. Прикладом NPoA є маршрутизатор доступу.

• Subnet - підмережа, яку обслуговує одним NPoA.

• Serving Area - зона обслуговування, яка може включати декілька підмереж, що обслуговуються одним APoA.

Функціональні елементи мережі IP-телефонії, що беруть участь при реалізації функцій мобільності, показані на рис.53.

У мережах IP-телефонії можливі наступні чотири сценарії мобільності.

1. Мобільність між підмережами.
2. Мобільність між зонами обслуговування.
3. Мобільність між підмережами і зонами обслуговування одночасно.
4. Мобільність між підмережами, що знаходяться в різних зонах обслуговування.

Рис.53. Функціональні елементи, залучені в обслуговування абонента при мобільності

На рис.54-57 показані різні сценарії мобільності абонента в мережі IP-телефонії.

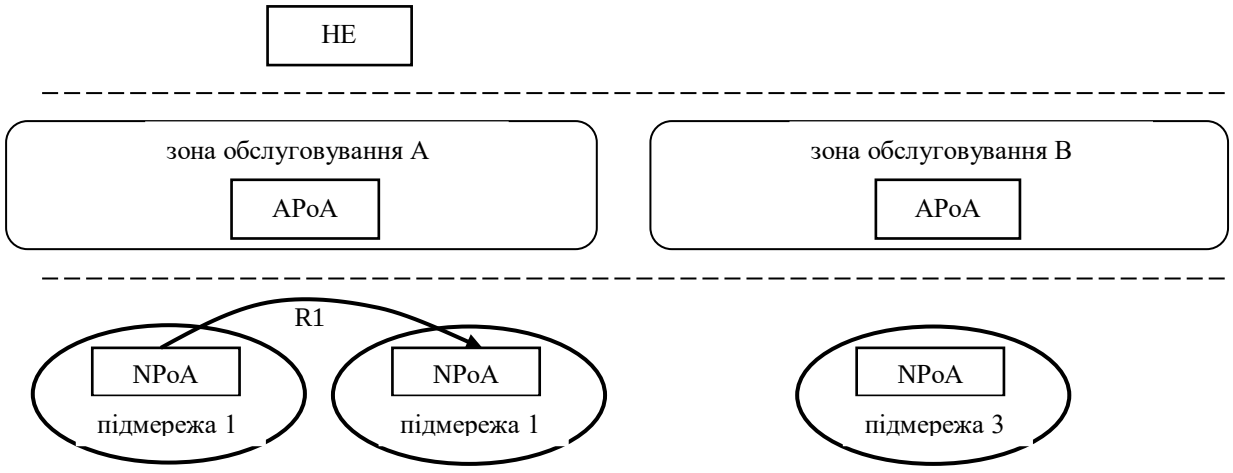

Рис.54. Мобільність між підмережами в межах однієї зони обслуговування

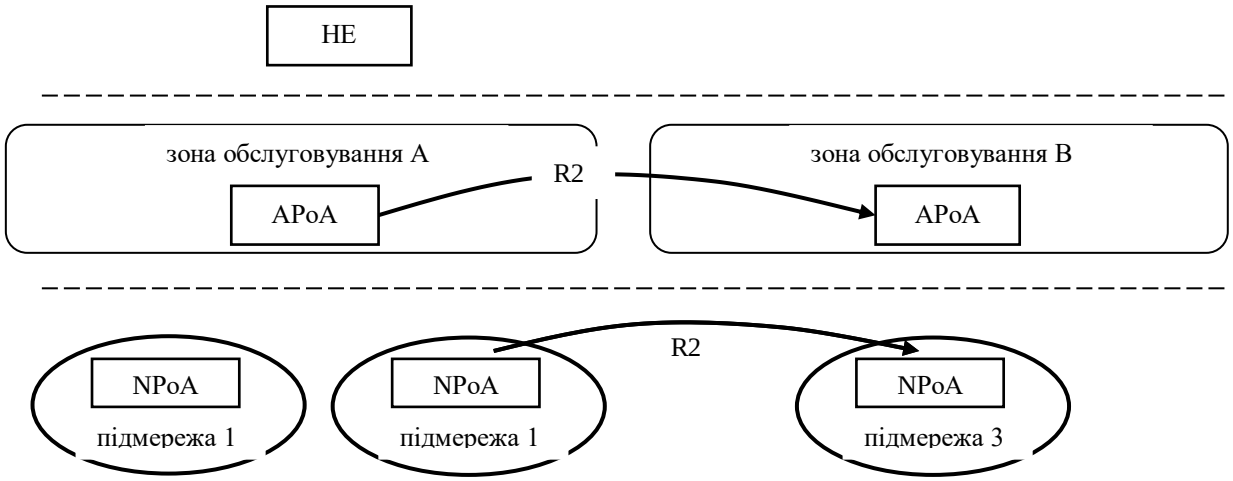

Рис.55. Мобільність між підмережами і між зонами обслуговування

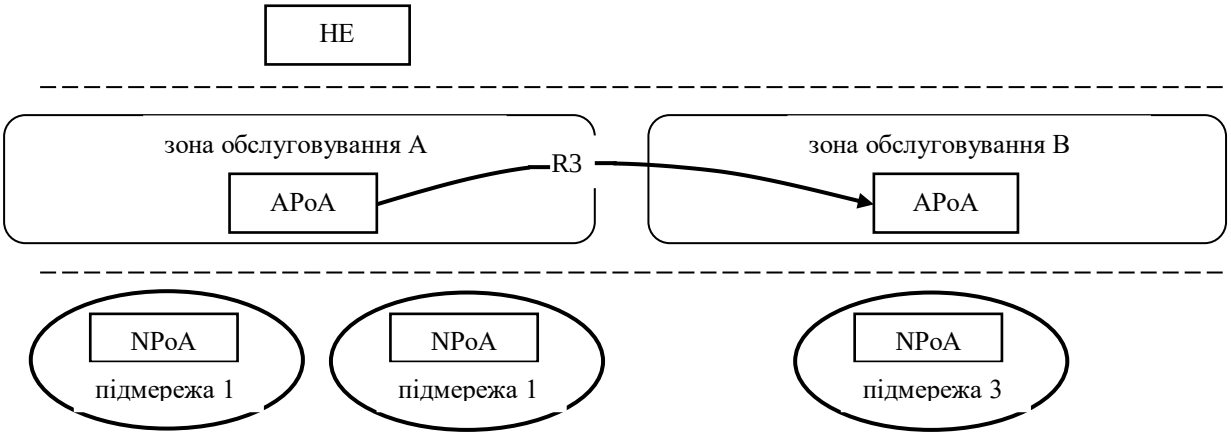

Рис.56. Мобільність між зонами обслуговування

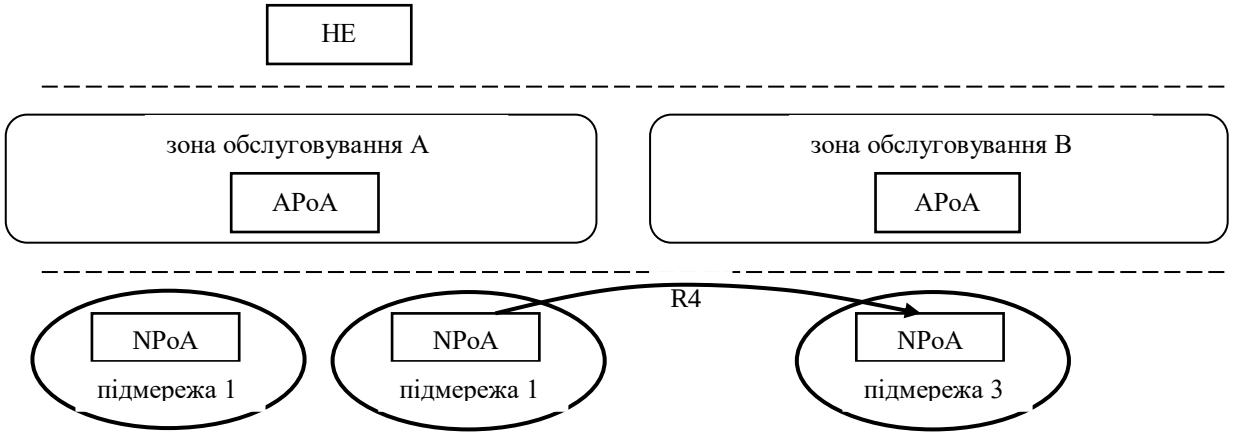

Рис.57. Мобільність між підмережами, що знаходяться в різних зонах обслуговування

7.4. Мобільність в мережі IP-телефонії на базі протоколу IPv4

У мережах 1P-телефонйі, побудованих на базі протоколу IPv4, термінал переміщається з однієї мережі в іншу не змінюючи свого IP адреси.

У процедурі мобільності беруть участь три компонента: мобільний термінал (МТ), домашній регістр і візітний регістр (рис.58).

Мобільний термінал - це термінал, який переміщається з однієї мережі в іншу.

Домашній регістр - це регістр, який зберігає всю необхідну інформацію про мобільному терміналі. Візитний регістр - це регістр, обслуговуючий зону, відмінну від зони домашнього регістра.

Функції родинної злагоди і візитною регістрів зазвичай виконуються маршрутизаторами.

Кореспондентський вузол - вузол в мережі IP-телефонії, обмінюються даними з мобільним терміналом.

У протоколі IP мобільний термінал може використовувати два IP адреси: один для ідентифікації - домашня адреса (home address) і один для маршрутизації - адреса обслуговування (care-of address). Існує два типи адреси обслуговування: суміщений адреса обслуговування (co-located care-of address) і адреса обслуговування візитною регістра (foreign agent care-of address). Поєднаний адреса обслуговування являє собою тимчасову адресу, який при- привласнювати самостійно вузлом або виходить безпосередньо з PPP або DHCP сервера. Адреса обслуговування визітного регістра - це адреса регістра, в якому зареєстрований мобільний термінал. У процедурах реєстрації мобільний термінал може використовувати суміщений адреса обслуговування або адреса обслуговування візитною регістра, проте використання суміщеного адреси призводить до зменшення дефіцитних ресурсів, а саме адрес IP, тому зазвичай використовується адреса обслуговування візитною регістра.

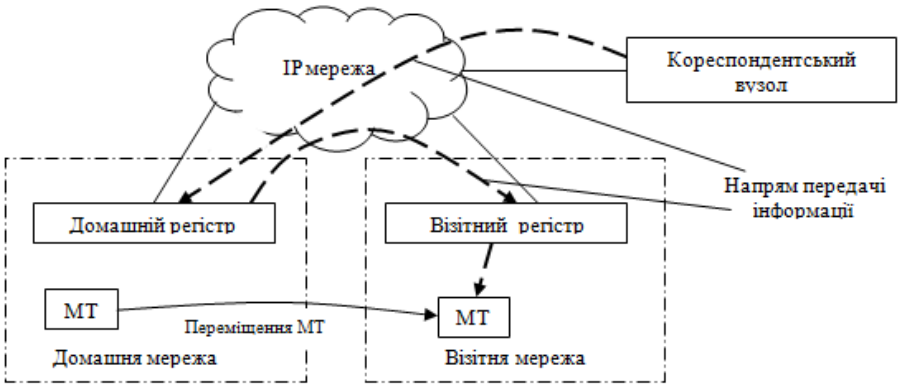

Рис.58. Приклад передачі інформації для мобільного терміналу в мережі на базі протоколу IPv4

Після того як мобільний термінал зареєструється в новій мережі, він посилає дані про адресу обслуговування домашньому регістру. Домашній регістр оновлює свої таблиці маршрутизації, створювати чи змінювати вже існуючи біллінгові записи і асоціює домашню адресу мобільного терміналу з його поточним адресою обслуговування.

Коли домашній регістр отримує дані, призначені для мобільного терміналу, він перенаправляє їх за адресою обслуговування цього терміналу, використовуючи метод інкапсулювання, також відомий як метод туннелірования. У зворотному напрямку мобільний термінал зазвичай посилає пакети через маршрутизатор візитною мережі. Таким чином, в протоколі IPv4 відсутня оптимізація маршруту до мобільного терміналу при його роумінгу.

7.5. Мобільність в мережі IP-телефонії на базі протоколу SIP

В даний час, в рамках досліджень IETF, розробляються нові протоколи, які підтримують персональну мобільність. Одним з таких протоколів є протокол ініціювання сеансу зв'язку (SIP). SIP - це прикладний протокол, який може встановлювати сеанси зв'язку мультимедіа або телефонні з'єднання і управлять ними. Мобільність користувача в цьому протоколі заснована на використанні унікального персонального ідентіфікатора.

Користувач вноситься в список сервера-реєстратора, після того як він надсилає запит про реєстрацію. Так-леї сервер-реєстратор повідомляє домашньому сервера користувача, де той зареєстрований.

Зухвалий користувач посилає повідомлення-запрошення для абонента, що викликається на найближчий проксі-сервер, який запитує у домашнього сервера поточне місце розташування абонента і, отримавши необхідну інформацію, надсилає повідомлення-запрошення на сервер-реєстратор, в якому зареєстрований визувати користувач. Абонент підтверджує отримання повідомлення-запрошення, після чого проксі-сервер встановлює з'єднання між користувачами.

Протокол SIP не розглядає мобільність термінального обладнання.

7.6. Реалізація функцій мобільності в стандарті H.323

Мобільність користувача IP-телефонії в стандарті H.323 можлива, але до кінця не визначена. У відповідності з процедурами стандарту спочатку встановлюється сигнальне з'єднання з gatekeeper зони H.323, отже, адреса абонента може бути визначений перед встановленням з'єднання, а, тому, можливо перенаправлення з повною обробкою на прикладному рівні.

Сучасний стан розробок дозволяє говорити про те, що підтримка мобільності

можлива і без додавання нових компонентів, і з мінімальними модифікаціями самого стандарту H.323. При цьому послуги мобільності IP-телефонії можуть бути додатковим сервісом в існуючих, що підтримують H.323 системах телефонного зв'язку Internet.

У поточній версії H.323 мобільність хост-машин забороняється, виходячи з основного механізму IP, який неявно передбачає, що хост-машина стаціонарна.

7.7. IP-телефонія для користувачів мереж стільникового рухомого зв'язку

Для того, щоб абоненти стільникових мереж могли скористатися послугами мереж передачі даних, була розроблено нова технологія GPRS, яка є складовою частиною системи GSM, однак може бути адаптована і під інші технології.

Інфраструктура мережі GSM / GPRS складається з інфраструктури мережі GSM і двох додаткових елементів: SGSN (вузол, що підтримує послуги GPRS) і GGSN (вузол, що виконує функції шлюзу GPRS).

SGSN виконує функції управління мобільністю і функції реєстрації абонентських даних, включаючи ідентифікатори і місцезнаходження користувача.

GGSN - це шлюз між системою GPRS і IP-мережею, який управляє взаємодією між мобільним користувачем і мережею.

Перш, ніж отримати доступ до послуг, мобільний користувач повинен зареєструватися в SGSN. При реєстрації користувача SGSN запитує його дані з HLR (домашнього регістра) або SGSN, де він був зареєстрований раніше.

Для передачі або прийому інформації мобільної станції необхідно активне PDP (Packet Data Protocol) з- єднання, яким керує GGSN. При взаємодії GGSN з мобільною станцією використовуються PDP адреси.

При обміні інформацією, призначеної для користувача, між SGSN і GGSN використовується GPRS Tunnelling Protocol (GTP).

Крім того, в стандарті GRPS, як і в GSM, забезпечення ідентифікації доступності мобільної станції і мобільність обслуговування між мережами, що підтримують GPRS. Як тільки мобільна станція переміщається в іншу мережу, інформація про профіль її обслуговування передається в SGSN візитною мережі.

У табл.8 приведена характеристика мобільності для GPRS.

Табл.8. Характеристика мобільності для технології GPRS

Критерії		**Мобільність GPRS**
Ідентифіка-тори	користувачів	IMSI
	терміналів	IMEI
	додатків	PDF адреса
	місцяположення	RAI, Cell ID
Критичні елементи протоколу		MS, SGSN, GGSN, HLR (VLR)
Можливості Handover		Так
Мобільні елементи, залучені в Handover		MS, SGSN (VLR)
Індикації стану		Так
Додаткові можливості	QoS	PDF
	кодек	
	безпека	
	Інше	
Оптимізація маршруту		Так
Транспортабельність послуг		Так

ЛІТЕРАТУРА

1. Девідсон, Джеймс Пітерс, Манож Бхатія, Сатіш Калідінді, Судіпто М. Основи передачі голосових даних по мережах IP (IP Voiceover IP Fundamentals); Вільямс, 2012.

2. Гепко И.А., Олейник В.Ф., Чайка Ю.Д., Бондаренко А.В. Современные сети: состояние и перспективы их развития. – К.: «ЕКМО», 2009. – 672с.

3. Григорьев В.А., Лагутенко О.И., Распаев Ю.А. Сети и системы. – М.: Эко-Трендз, 2005. – 345с.

4. Скляр Б. Цифровая связь. Теоретические основы и практическое применение: Пер. с англ. – М.: Изд. дом «Вильямс», 2004. – 104с.

5. Хоменок М.Ю., Данилевич А.В. Системы сигнализации в сетях телекоммуникаций: Учеб. пособие по курсу “Системы сигнализации в телекоммуникациях” для студентов специальности “Телекоммуникационные системы” - Мн.: БГУИР, 2000. – 112 с.

6. Дузь В.И. Системы коммутации и распределения информации. Учеб. пособ. / Дузь В.И., Соловская И.Н. – Одесса: ОНАС им. А.С. Попова, 2013. – 168 с.

7. Никитюк Л.А., Шерепа И.В. Телекоммуникационные и информационные сети: Навч. Посібник / за редакцією М.В. Захарченка.- Одеса: УДАЗ ім. О.С. Попова, 2000. – 112с.

8. Живиця М.І., Грохольський Я.М., Шелепенко Ю.В., Наталенко П.П., Савінов О.П., Троцько О.О. Телекомунікаційні мережі з комутацією пакетів. Навчальний посібник. – К.: ВІТІ НТУУ «КПІ», 2011. – 352с.

9. Гольдштейн Б.С. Сигнализация в сетях связи / Б.С. Гольдштейн; Т.1. Протоколы сети доступа. Т.2. – М.: Радио и связь, 2005.

10. Гольдштейн, Б.С. Протокол SIP / Б.С. Гольдштейн, А.А. Зарубин, В.В.Саморезов; Серия «Телекоммуникационные протоколы». – СПб. : БХВ – СПб, 2005.

11. Гольдштейн А.Б., Гольдштейн Б.С. SOFTSWITCH. СПб.: БХВ – Санкт-Петербург, 2006. – 368с.

12. Бакланов, И.Г. NGN: Принципы построения и организации / И.Г. Бакланов; под ред. Ю.Н. Чернышова. – М.: Эко-Трендз, 2008.

13. Росляков А.В., Самсонова М.Ю., Шибаев И.В. IP-телефония - М.: ЭкоТренд, 2007. – 252с.

14. Гольштейн Б.С., Пинчук А.В., Суховицкий А.Л.: IP-телефония - М.: Радиосвязь, 2009.- 366с.

15. Леинванд, Аллан, Пински, Брюс. Конфигурирование маршрутизаторов Cisco, 2-е изд. : Пер. с англ. — М. : Издательский дом "Вильяме", 2001. — 368 с.

16. Евсеенко Г.Н. Цифровые системы передачи: Учебное пособие. - Ростов-на-Дону: РКСИ, 2005. – 100с.

17. Атцик А.А. Протокол Megaco/H.248 / А.А. Атцик, А.Б. Гольдштейн, Б.С. Гольдштейн; Серия «Телекоммуникационные протоколы». – СПб. : БХВ – СПб, 2009.

18. Ткаленко О.М., Невдачина О.В. SIP-технологія в IP-мережах: навчальний посібник / О.М. Ткаленко, О.В. Невдачина // Київ: ДУТ, 2015.

19. Васин Н.Н. Построение сетей на базе коммутаторов и маршрутизаторов/ Н.Н. Васин. – М.: Национальный Открытый Университет «ИНТУИТ», 2016.