ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ТЕЛЕКОМУНІКАЦІЙ ТА ІНФОРМАТИЗАЦІЇ

СТОРЧАК К.П., ТКАЛЕНКО О.М., ПОЛОНЕВИЧ О.В., ЧОРНА В.М.

ТЕХНОЛОГІЇ ПРОГРАМНОЇ КОМУТАЦІЇ

НАВЧАЛЬНИЙ ПОСІБНИК

Київ - 2018

УДК 621.395.37
681.324
ББК 32.882

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

Навчальний посібник призначений для самостійної роботи студентів вищих навчальних закладів для поглибленого вивчення дисциплін «Системи комутації та розподілу інформації», «Технології програмної комутації» – циклу дисциплін професійної та практичної підготовки за спеціальностями 6.050903 Телекомунікації, 172 Телекомунікації та радіотехніка.

Сторчак К.П., Ткаленко О.М., Полоневич О.В., Чорна В.М. Технології програмної комутації. Навч. посібник, підготовлено для студентів вищих навчальних закладів – Київ: ДУТ, 2018. – 104с.

У посібнику представлені принципи програмної комутації, концептуальні основи 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 архітектурні системи IP-телефонії на базі Рекомендацій ITU-T H.323 і концепції TIPHON, що розроблена ETSI. Описані питання сигналізації, принципи протоколу SIP, інтеграція SIP з IP мережами. Наведено алгоритми встановлення SIP з’єднань, здійснено аналіз практичного використання протоколу SIP. Здійснено порівняльний аналіз протоколів H.323 та SIP.

Навчальний посібник призначений для студентів денної та заочної форм навчання за спеціальностями 6.050903 Телекомунікації, 172 Телекомунікації та радіотехніка, а також може бути корисним для аспірантів, викладачів навчальних закладів відповідних спеціальностей, фахівців, які обслуговують інформаційно-комунікаційні мережі зв’язку.

ЗМІСТ

ПЕРЕДМОВА

Телефонні мережі та мережі передавання даних співіснували протягом десятиріч і розвивалися незалежно одна від одної. І одні, і інші відповідно надавали свій незалежний спектр послуг. IP-телефонія об'єднує їх в єдину комунікаційну мережу, яка пропонує потужний та економічний засіб зв'язку. Можливість передавати голосовий трафік з фіксованою якістю по пакетним мережам передавання даних визначила подальший напрямок розвитку в області телефонії. Крім надавання послуг телефонного зв'язку, у межах мережі передавання даних (у тому числі мережі, що працює по протоколу IP), стало доступним здійснення транзиту голосового трафіку між вузлами PSTN/ISDN, а також встановлювати сеанси зв'язку за сценарієм «комп'ютер-телефон» і «телефон-комп'ютер».

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.

Набір рекомендацій H.323 – це спроба перенести телефонну сигналізацію ISDN Q.931 на IP-з'єднання, тобто «накласти» традиційну телефонію на мережі передавання даних. Набір рекомендацій H.323 не зміг забезпечити вагомі покращення для кінцевих користувачів. Вона не змогла стати основною ні для розробки нового покоління кінцевих точок, ні для підтримки додаткових видів обслуговування, які схожі за тими, що надають традиційні установчі системи комутації. Для того, щоб забезпечити реальні інновації на рівні кінцевих вузлів, індустрія повинна спростити процес розробки нових прикладень, запропонувавши для цього стандартні програмні інтерфейси та інструментарій високого рівня. Але, як показує розвиток засобів комп'ютерно-телефонної інтеграції, навіть цього недостатньо. Необхідно, щоб модель надавання телефонних послуг будувалася на базі служб мереж передавання даних – тоді вона дозволить швидко

розроблювати зручні і сумісні рішення для мереж NGN.

Впровадити розвинену підтримку мовних комунікацій в середовище передавання даних можна за допомогою протоколів, які орієнтовані в першу чергу на надавання послуг кінцевим користувачам. Створені на їх основі продукти повинні легко інтегруватися у існуючі мережі, вимагаючи лише мінімальної модифікації мережних інфраструктур, а самі протоколи – легко розширюватися, причому так, щоб додавання в них нових функцій не порушувало роботу систем, які основані на попередніх версіях, та не вимагало відповідного одобрення організаціями із стандартизації, які конкурують одна з одною. Всім цим критеріям відповідає протокол SIP (Session Initiation Protocol), який запропонований однією з робочих груп комітету IETF. Він регламентує алгоритми встановлення, модифікації і закінчення мультимедійних (у тому числі голосових) з'єднань. SIP багато перейняв у таких відомих протоколів, як HTTP та SMTP, які вже довели свою значимість.

Багато стандартів ніколи не втілюються в успішні комерційні продукти. До SIP це не відноситься. На ринку вже є шлюзи, сервери-посередники, термінали, які його підтримують. Впровадження протоколу SIP супроводжується роботою в подальшому розвитку та розширенню протоколу. Одне з можливих нових застосувань SIP – це використання його в якості протоколу встановлення з'єднання в стільникових мережах третього покоління (3G). Так, організація 3GPP (3rd Generation Partnership Project) вже прийняла його в якості сигнального протоколу рухомої мережі третього покоління. Ще одне застосування SIP – з'єднання АТС між собою за допомогою IP-тракту. В цьому випадку повідомлення протоколів ISUP, DSS-1 або QSIG інкапсулюються у повідомлення SIP.

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. SIP оснований на тому ж підході, що й HTTP: запит-відповідь (request-reply). Всі повідомлення SIP – текстові, їх можна

читати, а коди повернення – такі ж, як і в HTTP, тому деякі з них здаватимуться відомими не тільки адміністраторам мережі, але й багатьом користувачам Інтернету (404 – абонент не знайдений, 200 – ОК). Але після апробації протоколу на існуючих мережах і завдяки інтенсивному розвитку цього напрямку, початкова версія перенесла ряд змін. Частина вимог до реалізацій, які побудовані на новій версії протоколу SIP, не підтримує зворотної сумісності з реалізаціями, які виконані по початковій версії. У зв'язку з цим можуть виникнути ускладнення під час спроби встановлення взаємодії між пристроями, що виконані за різними версіями рекомендацій.

Крім нової версії протоколу, що описує загальні принципи роботи мережі, яка побудована з використанням технології на базі SIP, було специфіковано багато розширень сигнального протоколу, що доповнюють функціональні можливості логічних елементів SIP-архітектури, визначаючи механізми для надавання нових видів послуг та оптимізації алгоритмів взаємодії елементів у мережі.

1 ОСНОВИ ПРОГРАМНОЇ КОМУТАЦІЇ

1.1 Характеристика способів комутації абонентів у мережах

Сукупність телекомунікацій та вузлів, які їх з'єднують, що забезпечує взаємодію багатьох віддалених об'єктів, утворюють *телекомунікаційну мережу (Telecommunication Network).* В якості віддалених об'єктів при цьому можуть використовуватися як кінцеві системи інформаційної мережі, так і окремі локальні та територіальні мережі. Телекомунікаційна мережа виконує функції транспортної системи у складі інформаційної мережі, а інформаційні процеси породжують потоки рухомої інформації.

У загальному випадку під *інформаційною мережею* будемо розуміти сукупність територіально роззосереджених кінцевих систем, яка об'єднує їх телекомунікаційні мережі, забезпечує доступ прикладних процесів будь-якої із цих систем до всіх ресурсів мережі та їх сумісне використання.

Прикладний процес (Application Process) – це *процес у кінцевій системі мережі, який виконує обробку інформації для конкретної послуги зв'язку або прикладення.* Так, користувач, організуючи запит на надання тієї або іншої послуги, активізує у своїй кінцевій системі деякий *прикладний процес.*

Ресурси інформаційної мережі поділяються на *інформаційні,* ресурси *обробки та зберігання даних, програмні, комунікаційні* ресурси.

Інформаційні ресурси представляють собою інформацію та знання, які накопичуються у всіх галузях науки, культури та життєдіяльності суспільства, а також продукцію індустрії розваг. Все це систематизується у мережних банках даних, з якими взаємодіють користувачі мережі. Ці ресурси визначають цінність споживачів інформаційної мережі і повинні не тільки постійно створюватися і розширятися, але й своєчасно відновлюватися. Застарілі дані повинні знаходитися в архівах. Користування мережею забезпечує можливість отримувати актуальну інформацію тоді, коли виникає необхідність в ній.

Ресурси обробки і зберігання даних – це продуктивність процесорів мережних комп'ютерів та об'єми пам'яті їх запам'ятовуючих пристроїв, а також час, на протязі якого вони використовуються.

Програмні ресурси являють собою програмне забезпечення, яке бере участь у наданні послуг та прикладень користувачам, а також програми провідних функцій. До останніх відносяться: виписування рахунків, облік оплати послуг, навігація (забезпечення пошуку інформації в мережі), обслуговування мережних електронних поштових скриньок, організація мосту для телеконференцій, перетворення форматів інформаційних повідомлень, що передаються, криптозахист інформації (кодування і шифрування), аутентифікація (електронний підпис документів, який підтверджує їх справжність).

Комунікаційні ресурси – це ресурси, які беруть участь у транспортуванні інформації та перерозподілу потоків в комунікаційних вузлах. До них відносяться ємності ліній зв'язку, комутаційні можливості вузлів, а також час їх зайняття при взаємодії користувача з мережею. Вони класифікуються у відповідності з типом телекомунікаційних мереж: ресурси комутуємої телефонної мережі загального користування (КТМЗК), ресурси мережі передавання даних з комутацією пакетів, ресурси мережі мобільного зв'язку, ресурси наземної сповіщальної мережі, ресурси цифрової мережі інтегрального обслуговування (ЦМІО) і т.п.

Всі перераховані ресурси інформаційної мережі є *розподіленими,* тобто можуть використовуватися одночасно декількома прикладними процесами.

Телекомунікаційні мережі представляють собою комплекс апаратних та програмних засобів, які забезпечують передавання інформаційних повідомлень між абонентами з заданими параметрами якості. ***Повідомлення*** - форма представлення інформації, зручна для передавання на відстань. Повідомлення відображається зміною будь-якого параметру інформаційного сигналу (електромагнітні сигнали у мережах).

Комутація – процес з'єднання абонентів комунікаційної мережі через транзитні вузли (рис.1.1).

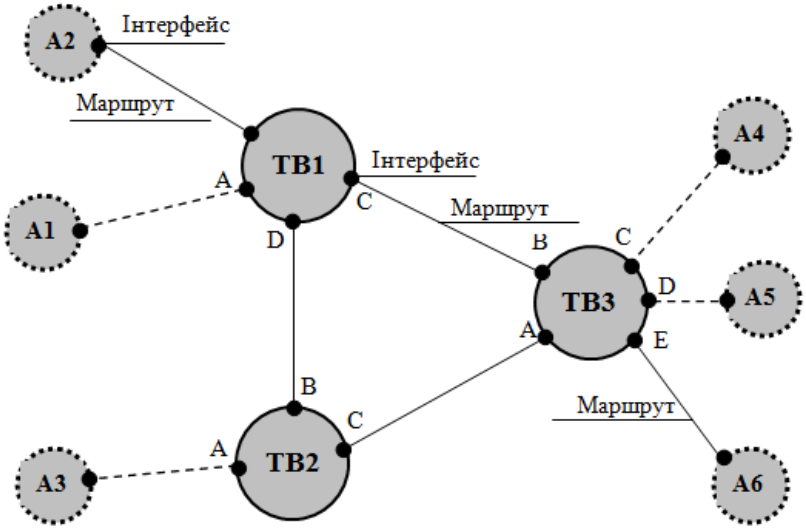


Рисунок 1.1 – Телекомунікаційна мережа

Комунікаційні мережі повинні забезпечувати зв’язок своїх абонентів між собою. Абонентами можуть виступати:

- ЕОМ;
- сегменти локальних мереж;
- факс-апарати;
- телефонні співрозмовники.

При створенні мереж телекомунікацій неможливо з’єднати всіх абонентів між собою окремими (виділеними) лініями зв’язку. Це недоцільно економічно і не підлягає виконанню практично. Тому з’єднання багатьох абонентів (А), які знаходяться на великій відстані, здійснюється через транзитні (телекомунікаційні) вузли (ТУ) зв’язку.

Таким чином, телекомунікаційна мережа утворюється сукупністю абонентів (А) та вузлів зв’язку, які з’єднані лініями (каналами) зв’язку. Вузли ТУ здійснюють комутацію повідомлення, яке надійшло, із вхідного порту (інтерфейсу) на вихідний. Наприклад, у мережі на рис.1 при передаванні повідомлення від абонента А2 абоненту А6 транзитний вузол ТУ1 здійснює комутацію повідомлення із вхідного інтерфейсу В на вихідний С, транзитний вузол ТУ3 – із вхідного інтерфейсу В на вихідний Е. При цьому формується визначений маршрут, по якому передається повідомлення. Процес формування маршруту отримав назву **комутація**. **Комутацією** також називають передавання

(просування) повідомлення із вхідного інтерфейсу на вихідний.

У деяких мережах всі можливі маршрути вже створені і необхідно тільки вибрати найбільш оптимальний. Процес вибору оптимального маршруту отримав назву **маршрутизація**, а пристрій, який її реалізує, - маршрутизатор. Вибір оптимального маршруту вузли здійснюють на основі таблиць маршрутизації (або комутації) з використанням визначеного критерію – метрики.

Оскільки у мережах загального доступу неможливо надати кожній парі абонентів власну фізичну лінію зв'язку, якою вони могли б монопольно володіти і використовувати у будь-який час, то в мережі завжди використовується певний ***спосіб комутації*** абонентів, що забезпечує розділення наявних фізичних каналів між декількома сеансами зв'язку та між абонентами мережі.

Основними способами комутації абонентів у мережах є:

1. *Комутація каналів (circuit switching);*
2. *Комутація повідомлень (message switching);*
3. *Комутація пакетів (packet switching).*

Таким чином, розрізняють мережі з *комутацією каналів*, коли телекомунікаційні вузли виконують функції комутаторів, і з *комутацією пакетів (повідомлень),* коли телекомунікаційні вузли виконують функції маршрутизаторів. У мережах з комутацією каналів канал створюється для передавання повідомлення.

1. *Комутація каналів* (КК, *circuit switching*) — організація складового каналу через декілька транзитних вузлів із декількох послідовно з'єднаних каналів на час передавання повідомлення (*оперативна комутація*) або на більш тривалий термін (*постійна/довготривала комутація*).

2. *Комутація повідомлень* (КС, *message switching*) — розбиття інформації на повідомлення, які передаються послідовно до найближчого транзитного вузла, який, прийнявши повідомлення, запам'ятовує його та передає далі таким же чином (конвейером).

3. *Комутація пакетів* (КП, *packet switching*) — розбиття повідомлення на «пакети», які передаються окремо. Різниця між повідомленням та пакетом: розмір

пакету обмежений технічно, повідомлення — логічно. При цьому, якщо маршрут просування пакетів між вузлами визначений раніше, говорять про *віртуальний канал* (із встановленням з'єднання). Приклад: комутація IP-пакетів. Якщо ж для кожного пакету завдання знаходження шляху вирішується заново, говорять про *датаграмний* (без встановлення з'єднання) *спосіб* пакетної комутації.

Кожний пакет облаштовується *заголовком*, в якому вказується як мінімум адреса вузла-отримувача та номер пакету. Передавання пакетів по мережі здійснюється незалежно один від одного. Комутатори такої мережі мають внутрішню буферну пам'ять для тимчасового зберігання пакетів, що дозволяє згладжувати пульсації трафіку на лініях зв'язку між комутаторами.

Відмінність комутації пакетів або повідомлень полягає в тому, що повідомлення може бути дуже великим. Тому, якщо в ньому виявляється помилка, повторно потрібно передавати всі повідомлення великого об'єму. У мережах з комутацією пакетів велике повідомлення попередньо розбивається на порівняно невеликі пакети (сегменти). Тому при втраті або спотворенні частини повідомлення повторно передається тільки втрачений пакет (сегмент).

4. *Комутація комірок* (КЯ, *cell switching*) — приватний випадок комутації пакетів з емуляцією віртуальних каналів (X.25, Frame Relay, MPLS), при комутації комірок пакети завжди мають фіксований і відносно невеликий розмір (Asynchronous Trasnfer Mode).

1.2 Принципи програмної комутації. Технологія комутованого Ethernet

Програмна комутація *використовує центральний процесор для здійснення примусової маршрутизації всіх пакетів та кожного окремо. Така комутація дозволяє маршрутизувати всі пакети та протоколи.*

Маршрутизатор – спеціалізований мережний комп`ютер, який має два та більше мережних інтерфейси, і який пересилає пакети даних між різними сегментами мережі. Маршрутизатор може з'єднувати різнорідні мережі різних архітектур.

Мережний інтерфейс – точка з'єднання між комп'ютером користувача та мережею; точка з`єднання двох мереж між собою.

Комутатор (Switch) – пристрій, який призначений для з`єднання декількох вузлів комп'ютерної мережі в межах одного сегменту мережі.

На рис.1.2 представлена ієрархічна модель мережі.

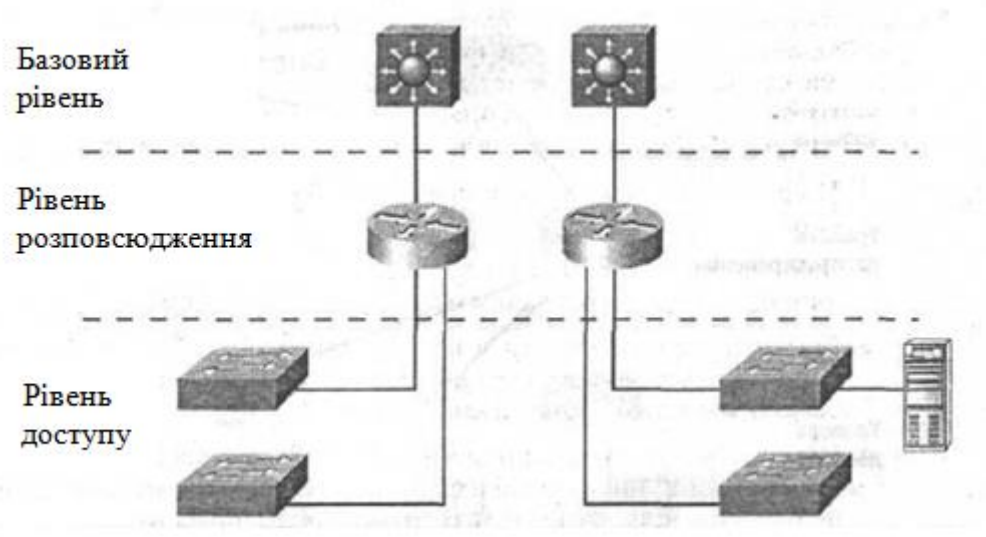


Рисунок 1.2 - Ієрархічна модель мережі

Рівень ядра відповідає за надійне і швидке передавання великих обсягів даних. Трафік, який передається через ядро, є загальним для більшості користувачів. Дані користувачів обробляються на рівні розподілу, який при необхідності, пересилає запити до ядра. Для рівня ядра велике значення має його відмовостійкість, оскільки збій на цьому рівні може призвести до втрати зв'язності між рівнями розподілу мережі.

Рівень розподілу (рівень робочих груп) є з'єднувальною ланкою між рівнями доступу та ядра. В залежності від способу реалізації, рівень розподілу може виконувати наступні функції: забезпечення маршрутизації, якості обслуговування і безпеки мережі; агрегацію адрес; перехід від однієї технології до іншої; об'єднання смуг пропускання низькошвидкісних каналів доступу у високошвидкісні магістральні канали.

Рівень доступу управляє доступом користувачів і робочих груп до ресурсів об'єднаної мережі. Основним завданням рівня доступу є створення точок входу/виходу користувачів в мережу. Рівень виконує наступні функції:

продовження (починаючи з рівня розподілу) управління доступом у мережі; створення окремих доменів колізій (сегментування); підключення робочих груп до рівня розподілу; рівень доступу використовує технологію комутуємих локальних мереж.

Технологія комутованого Ethernet використовує з'єднання «точка-точка», тому колізії відсутні. Для того, щоб можна було використовувати комутований Ethernet, потрібні мережні пристрої – комутатори (switch). Комутатор використовує повнозв'язну топологію із з'єднанням «кожний з кожним». Комутатор аналізує заголовок канального рівня, витягує звідти адресу отримувача і передає дані тільки одному комп'ютеру, якому вони призначені, а не всім комп'ютерам в мережі.

Рисунок 1.3 – Комутатор (switch)

Для розуміння логіки роботи комутатору необхідно розглянути *три особливості роботи комутаторів:*

1) Таблиця комутації

- Відповідність MAC-адрес портам комутатора

2) Алгоритм зворотного навчання

- Заповнення таблиці комутації

3) Алгоритм прозорого мосту

- Передавання кадрів комутатором

1) Комутатор знає MAC-адреси комп'ютерів, які підключені до його портів.

2) Про те, які комп'ютери підключені до портів комутатора, він дізнається за допомогою алгоритму зворотного навчання.

3) Після того, як таблиця комутації заповнена, комутатор використовує для передавання кадрів алгоритм прозорого мосту.

Розглянемо це більш детально (табл.1.1).

Таблиця 1.1 - Відповідність MAC-адрес портам комутатора

Порт комутатора	**MAC-адреса**
1	1C-75-08-D2-49-45
2	00-02-B3-A7-49-D1
3	00-04-AC-85-E7-03

Таблиця комутації містить відомості про MAC-адреси комп'ютерів, які підключені до портів комутатора. В найпростішому вигляді таблиця комутації містить всього 2 стовбці:

- порт комутатору;
- MAC-адресу комп'ютера, який підключений до цього порту.

Для розуміння логіки роботи комутатора достатньо всього два стовбці.

Для того, щоб дізнатися про MAC-адреси комп'ютерів, які підключені до портів комутатору, він використовує алгоритм зворотного навчання. Розглянемо, яким чином він працює (рис.1.4).

Припустимо, у нас є комутатор на 8 портів і в нього таблиця комутації. Комутатор тільки включився, при цьому таблиця комутації пуста (комутатор нічого не знає про комп'ютери, які до нього підключені). Комп'ютери підключаються до портів комутатору і починають передавати дані. Комутатор приймає всі кадри, які приходять на його порти.

Рисунок 1.4 – Алгоритм зворотного навчання

Припустимо, що прийшов кадр на третій порт. Далі комутатор аналізує

заголовок канального рівня (рис.1.5). Він витягує адресу отримувача, адресу відправника, тип протоколу наступного рівня. Комутатор аналізує адресу відправника і бачить там MAC-адресу 00-02-B3-87-A0-E6 і він розуміє, що до третього порту підключений комп'ютер з такою MAC-адресою. Тому комутатор бере цю MAC-адресу і записує її в таблицю комутації у рядок, який відповідає третьому порту. Наступного разу, коли прийдуть дані для комп'ютера з такою MAC-адресою, комутатор знає, що їх потрібно відправляти на третій порт.

Рисунок 1.5 - Алгоритм зворотного навчання

Тепер розглянемо роботу алгоритму прозорого мосту, який використовується комутаторами для передавання кадрів (рис.1.6).

Припустимо, що комутатор вже заповнив всю таблицю комутації і знає MAC-адреси комп'ютерів, які підключені до його портів. Приходить кадр на четвертий порт. Комутатор аналізує заголовок канального рівня, але зараз він витягує адресу отримувача і виконує пошук у таблиці комутації (рис.1.7).

Рисунок 1.6 – Алгоритм прозорого мосту

Комутатор бачить, що комп'ютер з такою MAC-адресою підключений до

другого порту. Тому комутатор передає кадр, який надійшов, на другий порт.

Рисунок 1.7 – Алгоритм прозорого мосту

Приходить наступний кадр (рис.1.8). Комутатор знову витягує адресу отримувача із заголовку канального рівня і виконує пошук у таблиці комутації.

Рисунок 1.8 – Принципи програмної комутації

Розглянемо, що відбувається, якщо приходить кадр, призначений для отримувача, MAC-адреси якого немає в таблиці комутації.

В цьому випадку, комутатор працює так само, як працює концентратор у класичному Ethernet (рис.1.9). Комутатор передає кадр на всі порти з надією на те, що до якого-небудь з цих портів підключений комп’ютер з такою MAC-адресою, просто можливо він не передавав поки що ніяких даних і комутатор про нього нічого не знає.

Рисунок 1.9 – Принципи роботи комутатору

Алгоритм прозорого мосту був розроблений для попередника комутатора - мережного мосту - і використовувався для об'єднання декількох мереж класичного Ethernet (рис.1.10). Було декілька мостів, але для комутаторів був вибраний режим прозорого мосту.

Особливості прозорого мосту:

1) Не помітний для мережних пристроїв, тобто немає власної MAC-адреси.

2) Не потребує налаштування. Можемо включити комутатор, підключити до нього комп'ютери і вони зразу зможуть передавати дані один одному через комутатор без будь-яких додаткових конфігураційних дій.

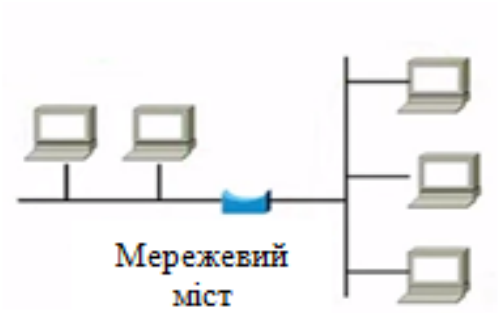


Рисунок 1.10 – Мережевий міст

Для порівняння маршрутизатор має власну IP-адресу на кожному інтерфейсі і йому необхідно сконфігурувати таблицю маршрутизації вручну або за допомогою якого-небудь протоколу маршрутизації.

При використанні тільки комутованого Ethernet колізії не виникають. Якщо до портів комутатора підключено по одному комп'ютеру, які працюють в режимі повний дуплекс (передають дані в прямому і в зворотньому напрямку), колізії виникнути не можуть.

Кадр (frame) Ethernet – структура, в яку включаються дані протоколів більш високого рівня.

MAC-адреса – фізична 48-бітова адреса пристрою (мережного інтерфейсу). Адреса складається з двух частин – 24-бітний ідентифікатор виробника та ідентифікатор пристрою.

Приклад: 00-1E-58-9E-C0-CB

24-бітова частина виробника (Vendor part)

24-бітовий ідентифікатор пристрою

Спеціальні MAC-адреси:

Широкомовна – FF-FF-FF-FF-FF-FF

Багатоадресна – 01-xx-xx-xx-xx-xx

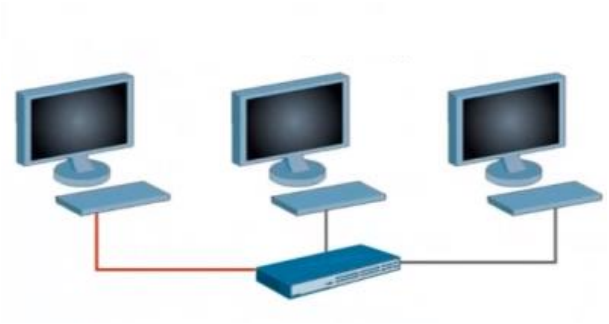


Рисунок 1.11 – Комутація кадрів

На рис.1.11 є комутатор, який передає кадр тільки у порт призначення. Передавання у порт призначення здійснюється тільки для одноадресних кадрів і тільки в тому випадку, якщо в таблиці комутації вже вивчена фізична адреса отримувача. Розглянемо детально роботу комутатора. Дані аналогічні з прикладом ретрансляції, але відмінність полягає в тому, що в схемі бере участь комутатор і він тільки що включений, тобто таблиця комутації не сформована.

Комутатор приймає кадр з адресою призначення хоста С і адресою джерела хоста А у свій перший порт. Аналізуючи заголовок, комутатор зразу додає адресу хоста А з прив`язкою до першого порту в таблиці комутації, а потім шукає в ній відповідність для хоста С. Оскільки такої відповідності у таблиці не має, то комутатор розсилає кадр у всі свої порти (рис.1.12).

Таблиця комутації	
MAC-Address	**Port**
00-1E-58-00-00-01	1

Заголовок кадру	
…	…
Dst MAC	00-1E-58-00-00-03
Src MAC	00-1E-58-00-00-01
…	…

Обробка кадру
• Приймаємо кадр з порту 1
• Записуємо відповідність Src MAC і порту
• Знаходимо відповідність для Dst MAC
• Надсилаємо кадр на всі порти

Рисунок 1.12 – Принципи комутації

Хост призначення прийме цей кадр і відправить якісь дані у відповідь (рис.1.13). Комутатор прийме цей кадр-відповідь з 3-го порту і запам`ятає в таблиці комутації відповідність порта 3 і адреси хоста С. Потім у відповідності з таблицею комутації цей кадр буде переданий через перший порт. З цього моменту всі кадри, які адресовані хостам А і С, будуть передаватися вже безпосередньо у порт призначення.

Таблиця комутації	
MAC-Address	**Port**
00-1E-58-00-00-01	1
00-1E-58-00-00-03	3

Заголовок кадру	
…	…
Dst MAC	00-1E-58-00-00-01
Src MAC	00-1E-58-00-00-03
…	…

Обробка кадру
• Приймаємо кадр з порту 3
• Записуємо відповідність Src MAC і порту

• Знаходимо відповідність для Dst MAC
• Надсилаємо кадр на порт 1

Рисунок 1.13 – Принципи комутації

Управляємі комутатори – підтримують широкий набір функцій управління і налаштування, які включають Web-інтерфейс управління, інтерфейс командного рядку (CLI), Telnet, SNMP, TFTP та ін. *Неуправляємі комутатори* – функції управління і налаштування не підтримують. *Комутатори, що налаштовуються* - займають проміжне положення між управляємими та неуправляємими комутаторами. Дозволяють виконувати налаштування визначених параметрів, але не підтримують віддалене управління по SNMP і Telnet. *L2-комутатори* - функціонують на другому рівні OSI; передають трафік із порта у порт або із VLAN у VLAN на основі MAC-адрес; розуміють тільки свою MAC-адресу; мають апаратну комутацію, високу продуктивність, оскільки пакет даних не підлягає змінам; виконують первинне сегментування мережі; не вміють маршрутизувати трафік; використовуються в якості комутаторів рівня доступу; мають найменшу вартість порту і ідеально підходять для підключення користувачів до мережі. *L3-комутатори* - приймають рішення на основі інформації мережного рівня, а не на основі MAC-адрес, але в основі комутації 3-го рівня лежить апаратна реалізація; використовуються для зв`язку між сегментами мережі і дозволяють маршрутизувати трафік між сегментами мережі (використовуються для маршрутизації трафіку у локальній мережі між існуючими сегментами, але не в назовні); використовуються як комутатори рівня розподілу.

Комутатори можна класифікувати по методам передавання кадрів. При ***комутації з проміжним зберіганням (store-and-forward)*** – комутатор копіює весь кадр у буфер і тільки потім його передає. Перед відправленням фрейму читаються його адреса призначення і адреса джерела, і тільки після цього кадр передається на вихідний порт. Цей спосіб передавання пов`язаний із затримками, при цьому, чим більше кадр, тим більше часу потрібно на його прийом. Під час прийому кадру здійснюється його перевірка на наявність помилок. ***Комутація «на льоту»***

(cut-through) – комутатор локальної мережі копіює у внутрішні буфери тільки адресу приймача (перші 6 байт після префіксу) і зразу починає передавати кадр, не дочекавшись його повного прийому. Цей режим зменшує затримку, але перевірка на помилки в ньому не виконується. Існують дві форми комутації «на льоту»: ***комутація із швидким передаванням (fast-forward switching)*** – ця форма комутації пропонує низьку затримку за рахунок того, що кадр починає передаватися негайно, як тільки буде прочитана адреса призначення. ***Комутація із вільними фрагментами (fragment-free switching)*** – фільтрує кадри з колізією перед їх передаванням. Цей метод комутації очікує, поки отриманий кадр не буде перевірений на предмет колізії і тільки після цього почне його передавання.

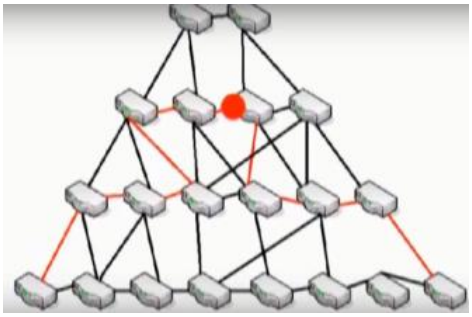
Основним критерієм вибору пристрою повинна бути відповідність можливостей пристрою бізнес-вимогам. Наприклад, необхідна підтримка IP, віртуальних приватних мереж (VPN). До інших характеристик можна віднести щільність (кількість) портів та швидкість інтерфейсу. Чим вище клас пристрою, тим вище щільність і швидкість. Попередньо потрібно вияснити технічні вимоги у місцевого провайдера регіональної мережі. При виборі комутатору потрібно зразу вирішити, чи буде пристрій працювати з настольними системами 10/100 або 1000 Мбіт/с, або чи буде застосовуватися для зв`язку інших комутаторів. Наступний критерій вибору – це щільність портів. Моделі початкового рівня мають не менше 12 портів, а високоякісні моделі підтримують сотні комутуємих портів в одному пристрої.

Трирівнева модель дозволяє вибрати тип пристрою (комутатору, маршрутизатору) для об`єднаної мережі.

1.3 Маршрутизація в IP-мережах

Представимо собі велику організацію з множиною підмереж і комп’ютерів-шлюзів. Наприклад, комп’ютеру А потрібно зв’язатися з комп’ютером Б. Сигнал може піти за замовчуванням по найкоротшому шляху. Але це з’єднання може бути повільним і сигнал піде в обхід, де обладнання буде новішим і швидшим (рис.1.14), швидкість з’єднання зросте. Сигнал також може і зовсім пройти безліч

шлюзів, перед тим як надійде до адресата. Питання в тому, яким чином сигнал доставити швидше.



А Б

Рисунок 1.14 – Підмережі і комп’ютери-шлюзи

Існують спеціальні алгоритми, які основані на мережних протоколах маршрутизації. *Протокол маршрутизації* – мережний протокол, який використовується маршрутизаторами для визначення можливих маршрутів передавання даних у складовій комп’ютерній мережі. Використання протоколу маршрутизації дозволяє уникнути ручного введення всіх допустимих маршрутів, що в свою чергу, зменшує кількість помилок, забезпечує узгодженість дій всіх маршрутизаторів в мережі і полегшує працю.

Дистанційно-векторні протоколи:

- RIP – Routing Information Protocol;
- IGRP – Interior Gateway Protocol;
- BGP – Border Gateway Protocol;
- EIGRP – Enhanced Interior Gateway Routing Protocol.

Протоколи стану каналів зв’язку:

- IS-IS – Intermediate System to intermediate System (стек OSI);
- OSPF – Open Shortest Path First;
- NLSP – NetWare Link-Services Protocol;
- HSRP і CARP – протоколи резервування шлюзу в Ethernet-мережах.

Основні переваги додавання маршруту самостійно:

1) Легкість налагодження і конфігурування в малих мережах.

2) Відсутність додаткових накладних витрат (із-за відсутності протоколів маршрутизації).

3) Миттєва готовність.

4) Низьке навантаження на процесор маршрутизатора.

5) Передбачуваність у кожний момент часу.

Маршрутизатор – це спеціалізований пристрій для об'єднання мереж. Маршрутизатори вміють узгоджувати відмінності в мережах. Маршрутизатор має декілька портів, які підключені до різних мереж. Кожний порт має IP-адресу в цій мережі. Для порівняння, комутатор власних IP-адрес не має. Для того, щоб об'єднати мережі, необхідно використовувати маршрутизатори. Неможна мережу 1 (рис.1.15) підключити до мережі 4 і передавати дані, обов'язково потрібний маршрутизатор на межі мереж.

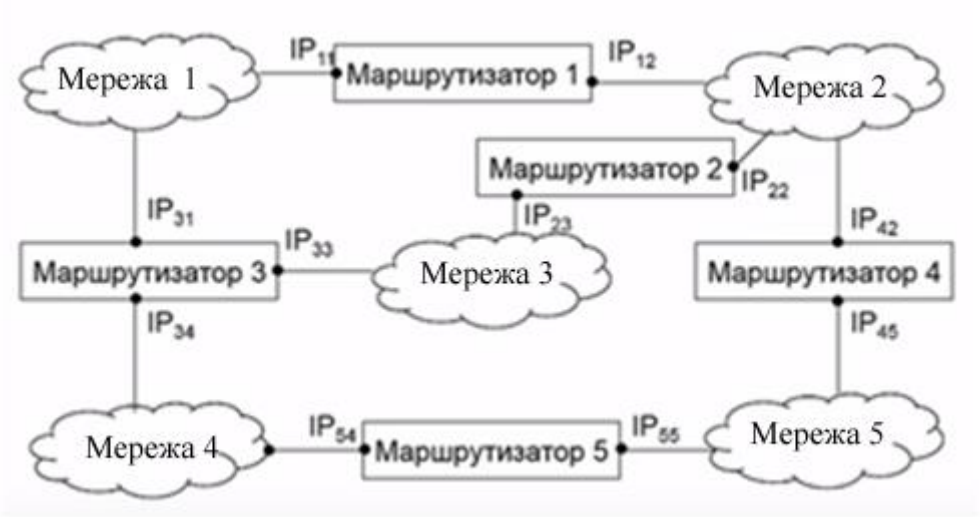


Рисунок 1.15 – Місце маршрутизаторів у мережі зв'язку

Основна функція, яку вирішують маршрутизатори – це *маршрутизація*.

При цьому ми повинні враховувати зміни в топології мережі: можуть з'являтися нові маршрутизатори, нові канали зв`язку, деякі маршрутизатори або канали зв'язку можуть виходити з ладу. Це все потрібно враховувати при пошуку маршруту.

Маршрутизація працює на мережному рівні моделі OSI. Маршрутизація – це пошук маршруту доставки пакету між мережами через транзитні вузли – маршрутизатори. Етапи маршрутизації:

- вивчення мережі;
- просування пакетів на маршрутизаторі.

Рисунок 1.16 – Складові мережі

На I етапі ми дізнаємося, які мережі у нас є в нашій складовій мережі, які є маршрутизатори і як вони пов`язані між собою.

На II етапі, коли на маршрутизатор надходить пакет, він приймає рішення куди цей пакет відправити: на який з інтерфейсів і в яку мережу (рис.1.17).

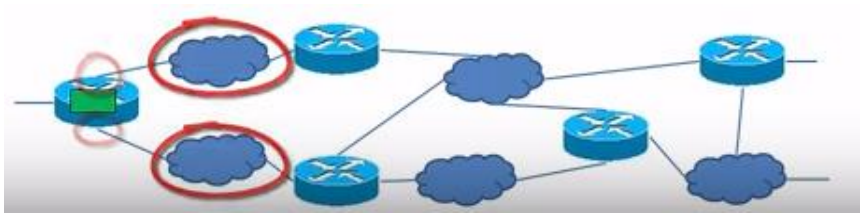


Рисунок 1.17 – Рішення маршрутизатору з відправлення пакету

Почнемо з другого етапу. Розглянемо, яким чином маршрутизатор визначає, куди відправляти пакет. Цей процес є простішим для розуміння. Потім ми перейдемо до того, як маршрутизатори вивчають мережу.

Маршрутизацію будемо вивчати на прикладі складової мережі (рис.1.18). Є декілька мереж, які об`єднаються декількома маршрутизаторами. Припустимо, що на маршрутизатор D прийшов пакет і йому потрібно вирішити, що робити з цим пакетом. В залежності від того, якій мережі призначений пакет, маршрутизатор може виконувати різні дії.

1ий варіант: пакет призначений для мережі, яка під`єднана безпосередньо до маршрутизатора, наприклад, мережа 10.1.0.0. В цьому випадку маршрутизатор передасть пакет прямо в цю мережу, яка до нього під`єднана.

2ий варіант: пакет призначений для мережі 10.3.1.0, яка приєднана не до маршрутизатора, але маршрутизатор знає, де ця мережа знаходиться. В цьому випадку маршрутизатор передасть пакет наступному маршрутизатору, який може продовжити доставку.

3^{ій} варіант: пакет призначений для мережі, про яку він нічого не знає. В цьому випадку маршрутизатор відкидає пакет. *В цьому полягає суттєва відмінність*

роботи маршрутизатора від роботи комутатора. Якщо комутатор не знає, куди відправити кадр, то він передає його на всі інтерфейси. Маршрутизатор так не робить, оскільки ми дуже швидко переповнимо складову мережу непотрібними пакетами. Для того, щоб знати, куди відправляти пакет, маршрутизатору потрібна наступна інформація:

- по-перше, у маршрутизатора є декілька інтерфейсів, до яких підключені різні мережі. Потрібно вирішити, в який з цих інтерфейсів відправити пакет;
- по друге, потрібно визначитися, що далі робити з цим пакетом. Можна відправити пакет у приєднану мережу або на якийсь з маршрутизаторів, які підключені до цієї приєднаної мережі. Якщо ми відправляємо на маршрутизатор, ми повинні знати IP-адресу цього маршрутизатора (10.1.0.19).

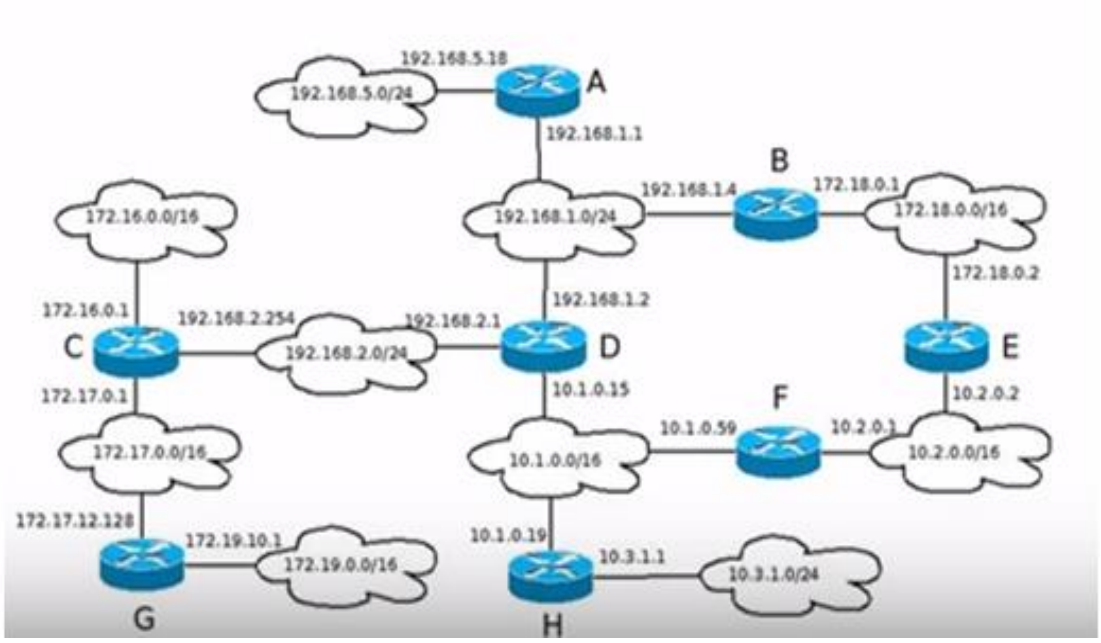


Рисунок 1.18 – Варіанти дій маршрутизатора

Всю необхідну інформацію маршрутизатор зберігає в таблиці маршрутизації (табл.1.2). Вона містить наступні стовбці: адреса, маска (вони й задають адресу мережі, в яку направлений пакет), шлюз, інтерфейс і метрика. На слайді приведений вид таблиці маршрутизації в ОС Windows, яка в якості номеру інтерфейса використовує IP-адресу, що призначена цьому інтерфейсу (192.168.1.2).

Таблиця 1.2 – Таблиця маршрутизації

Адреса	Маска	Шлюз	Інтерфейс	Метрика
192.168.1.0	255.255.255.0	Під’єднаний	192.168.1.2	276
192.168.2.0	255.255.255.0	Під’єднаний	192.168.2.1	276
10.1.0.0	255.255.0.0	Під’єднаний	10.1.0.15	276
172.16.0.0	255.255.0.0	192.168.2.254	192.168.2.1	306
10.2.0.0	255.255.0.0	10.1.0.59	10.1.0.15	306

Стовбець «Шлюз» може містити 2 варіанти значень. Якщо мережа приєднана безпосередньо до маршрутизатора (наприклад, 192.168.1.0/24, 192.168.2.0/24, 10.1.0.0/16), то у стовбці «Шлюз» буде так і написано, що мережа приєднана (on-link). Інший варіант значення у полі шлюз – це адреса наступного маршрутизатора, якому потрібно передати дані для доставки в мережу. Наприклад, якщо ми відправляємо дані в мережу 172.16.0.0/16, яка не приєднана до маршрутизатора (адреса: 172.16.0.0, маска: 255.255.0.0), нам потрібно передавати їх на наступний маршрутизатор (вказується його адреса: 192.168.2.254 у стовбці «Шлюз») і ми повинні вийти через інтерфейс 192.168.2.1. Якщо ми хочемо відправити дані в іншу мережу (наприклад, 10.2.0.0/16), інтерфейс буде інший (адреса: 10.2.0.0, маска 255.255.0.0, інтерфейс 10.1.0.15) і шлюз також буде відрізнятися (10.1.0.59).

Може виникнути деяке ускладнення: що писати в таблицю маршрутизації, якщо мережа, куди нам потрібно відправити дані, підключена не до наступного маршрутизатора, а знаходиться через один, через два або через три маршрутизатора (наприклад, мережа 172.19.0.0/16). Але при складанні таблиці маршрутизації нас це не повинно стосуватися. В таблиці маршрутизації ми повинні вказати адресу наступного маршрутизатора. Більше ми не вказуємо нічого, незалежно від того підключена мережа до маршрутизатора напряму або там є ще більша кількість проміжних маршрутизаторів. Вважаємо, що далі пересиланням буде займатися маршрутизатор С. Він вкаже наступний маршрутизатор, а той – наступний і т.д.

Розглянемо наступний варіант. У маршрутизатор D надійшов пакет, який призначений для мережі 10.2.0.0/16. До цієї мережі є два маршрути: напряму через маршрутизатор F, а також через 2 маршрутизатори B та E. Виникає питання, який з цих шляхів вибрати?

В таблиці маршрутизації допускається наявність двух і більше шляхів до однієї і тієї ж мережі (рис.1.19). В цьому полягає ще одна відмінність від комутаторів, де не допускається петель і кілець. І для того, щоб визначити, який з маршрутів вибрати, ми використовуємо поле «Метрика».

Таблиця 1.3 – Метрика

Адреса	Маска	Шлюз	Інтерфейс	Метрика
10.2.0.0	255.255.0.0	10.1.0.59	10.1.0.15	306
192.168.2.0	255.255.255.0	192.168.1.4	192.168.1.4	336

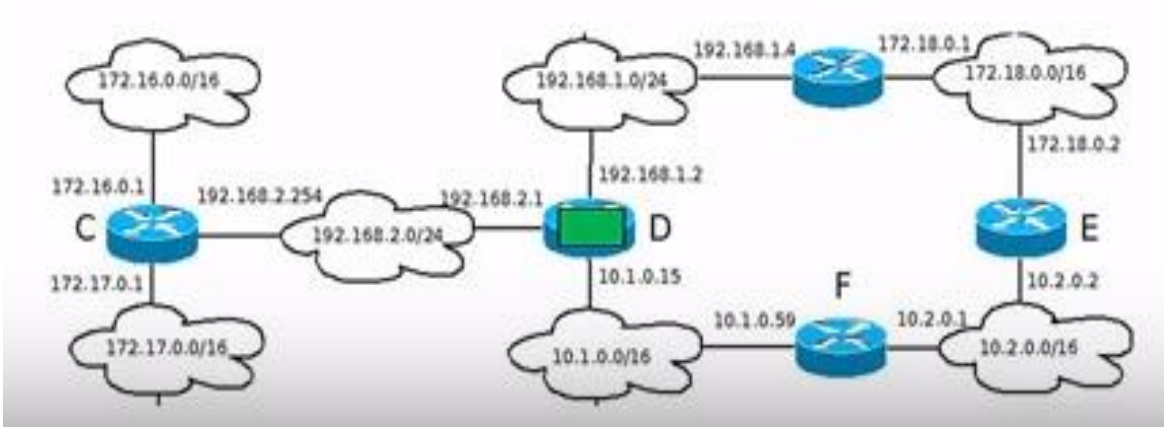


Рисунок 1.19 – Вибір шляху для просування пакету

Метрика – це вартість маршруту в деяких умовних одиницях. Вибираємо маршрут з мінімальною метрикою. Раніше в якості метрики використовувалася кількість маршрутів між мережами. В такому випадку маршрут через маршрутизатор F мав би метрику 1, а через маршрутизатори B та E мав би метрику 2. Зараз для складання метрики використовується більш складний підхід. Він основується не тільки на кількості маршрутизаторів, але й на швидкості, каналах зв`язку, які використовуються для підключення мереж і маршрутизаторів, на завантаженні цих каналів зв`язку.

Записи в таблиці маршрутизації можуть виникати двома шляхами: *статичним* (конфігурація інтерфейсів, прописування маршрутів до мереж вручну) та

динамічним (конфігуруються автоматично, протоколи маршрутизації RIP, OSPF, BGP та ін.).

Якщо використовується ***статична*** конфігурація, то всі записи в таблицю маршрутизації вносяться вручну адміністратором.

При ***динамічній*** маршрутизації записи в таблицю маршрутизації вносяться автоматично за допомогою протоколів маршрутизації. Перевагою динамічної маршрутизації є те, що вона відслідковує зміни в мережі. Якщо вийшов з ладу якийсь маршрутизатор, канал зв`язку або навпаки з`явився новий маршрут між мережами, то протоколи маршрутизації виявлять цю зміну і внесуть відповідні зміни в таблицю маршрутизації.

Якщо маршрутизатор отримав пакет для мережі, для якої в нього немає запису в таблиці маршрутизації, він відкидає такий пакет. Виходить, що для успішної роботи маршрутизатор повинен знати маршрути до всіх мереж у всій мережі Інтернет. На практиці це неможливо. Тому використовується маршрут за замовчуванням – це адреса маршрутизатора, на яку відправляються всі пакети для невідомих мереж. Умовне позначення маршрутизатора за замовчуванням 0.0.0.0 і маска 0.0.0.0 або пишеться слово default.

Всі сучасні маршрутизатори використовують ***швидку комутацію*** (***fast switching***). Така технологія забезпечує більш швидке передавання даних за рахунок різних методів кешування на програмній основі.

1.4 Технологія передавання голосової інформації з використанням протоколу IP - Voice over IP (VoIP)

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 дозволяє використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP (наприклад, мережу Інтернет) 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.

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.1.20), 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.

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.

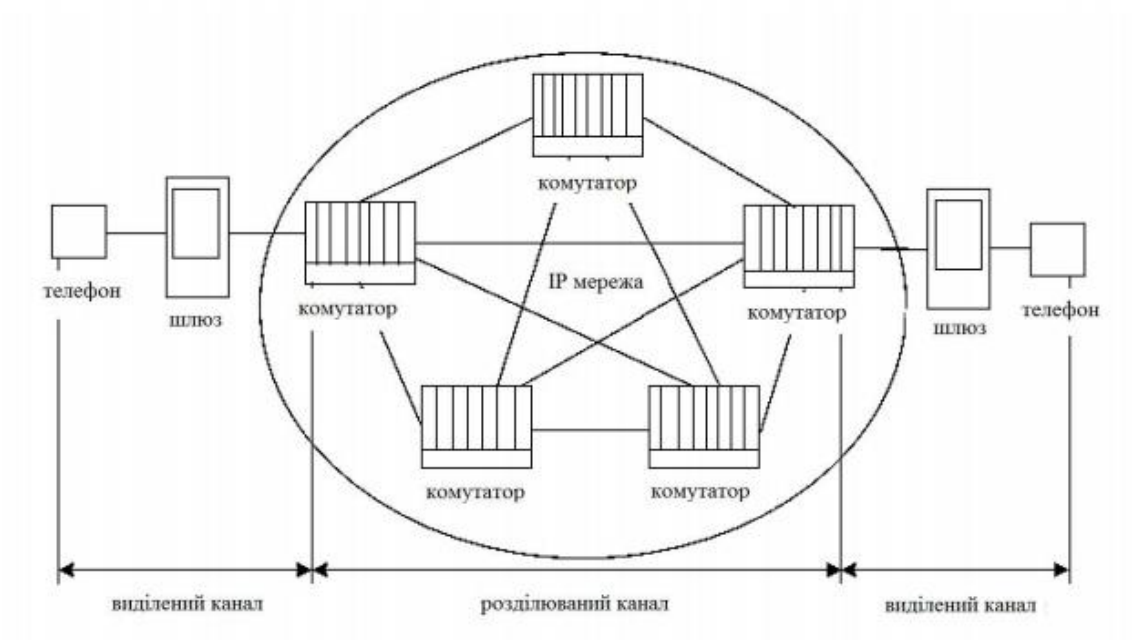


Рисунок 1.20 – З’єднання в мережі з комутацією пакетів

Отримана таким чином (не відновлена!) послідовність даних деком пресується 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.

Види з'єднань у мережі IP-телефонії

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

1. ***«Від телефону до телефону»*** (рис.1.21). 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.

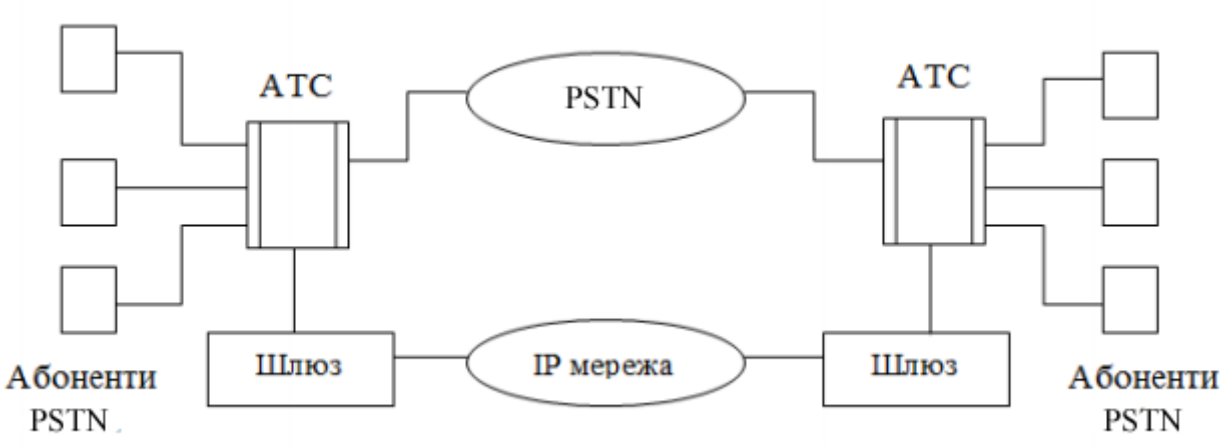


Рисунок 1.21 – Схема зв'язку «телефон-телефон»

2. **«Від комп'ютера до телефону»** (рис.1.22). 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.

Рисунок 1.22 – 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.1.23). 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.

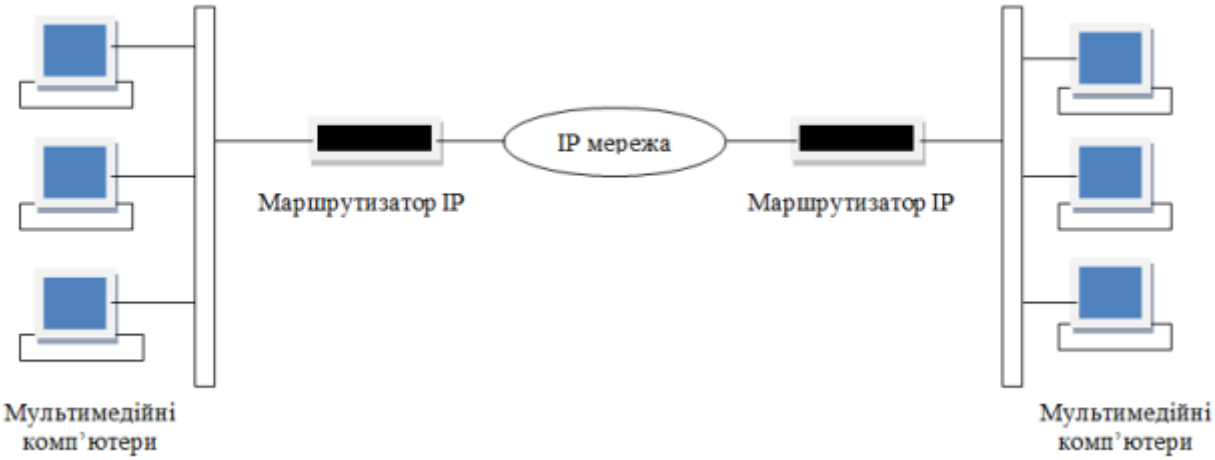


Рисунок 1.23 – Схема зв'язку «комп'ютер- комп'ютер»

4. **«Від WEB браузера до телефону»** (рис.1.24). 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.

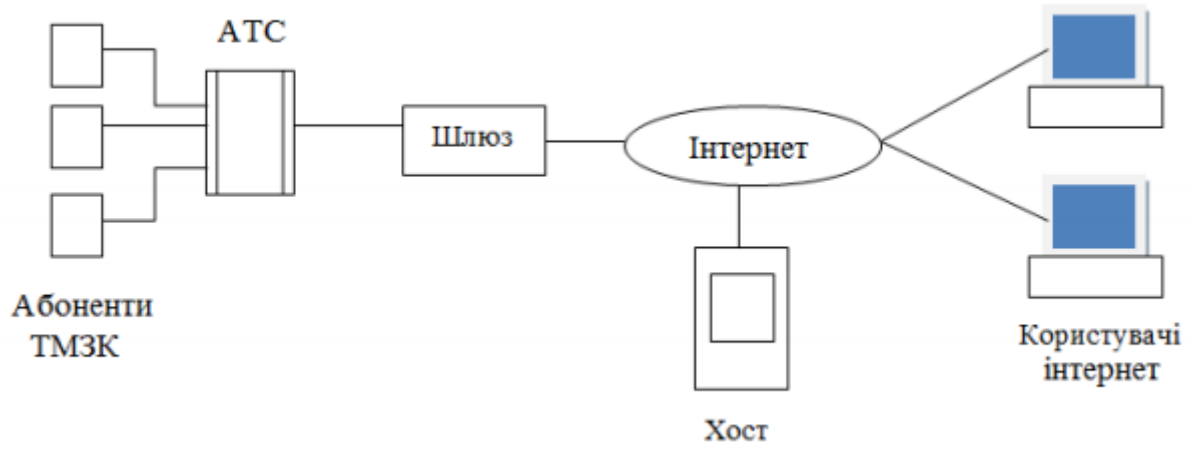


Рисунок 1.24 - Схема зв’язку «WEB-браузер- телефон»

Кінцевий користувач IP-телефонії отримує наступні додаткові переваги:

- більш низькі ціни на послуги телефонного зв’язку;
- підтримка голосу та даних;
- 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;
- доступ до нових послуг (голосова пошта, конференцзв’язок, передавання факсу та ін.) через відкритий інтерфейс архітектури на базі IP, що забезпечує сумісність для широкого спектру розробників прикладень;
- можливість налаштування набору послуг;
- простота оплати послуг IP-телефонії;
- простота контролю користувачем стану його розрахункового рахунку (через мережу Інтернет).

Контрольні запитання для самооцінки рівня знань

1. Які існують ресурси інформаційної мережі?
2. Якими бувають абоненти комунікаційних мереж?
3. У чому полягають принципи програмної комутації?
4. Які рівні включає ієрархічна модель мережі?
5. У чому полягають особливості роботи комутаторів?
6. Яким чином класифікують комутатори мереж зв’язку?
7. У чому полягають принципи маршрутизації в IP-мережах?
8. Яким чином класифікуються протоколи маршрутизації?
9. Яких типів буває маршрутизація?
10. Які існують види з’єднань у мережах IP-телефонії?
11. Які існують способи комутації абонентів у мережах?
12. У чому полягають особливості технології комутованого Ethernet?
13. Адресація яких типів використовується в IP-мережах?
14. У чому відмінність L2 та L3 комутаторів?
15. Особливості комутації з проміжним зберіганням?
16. Особливості комутації із швидким передаванням?
17. Особливості комутації із вільними фрагментами?

2 АРХІТЕКТУРА СИСТЕМ IP-ТЕЛЕФОНІЇ

2.1 Архітектура системи на базі стандарту H.323

Основною метою розробки стандарту H.323 стало забезпечення взаємодії з іншими типами мереж мультимедіа-зв’язку (рис.2.1). 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.

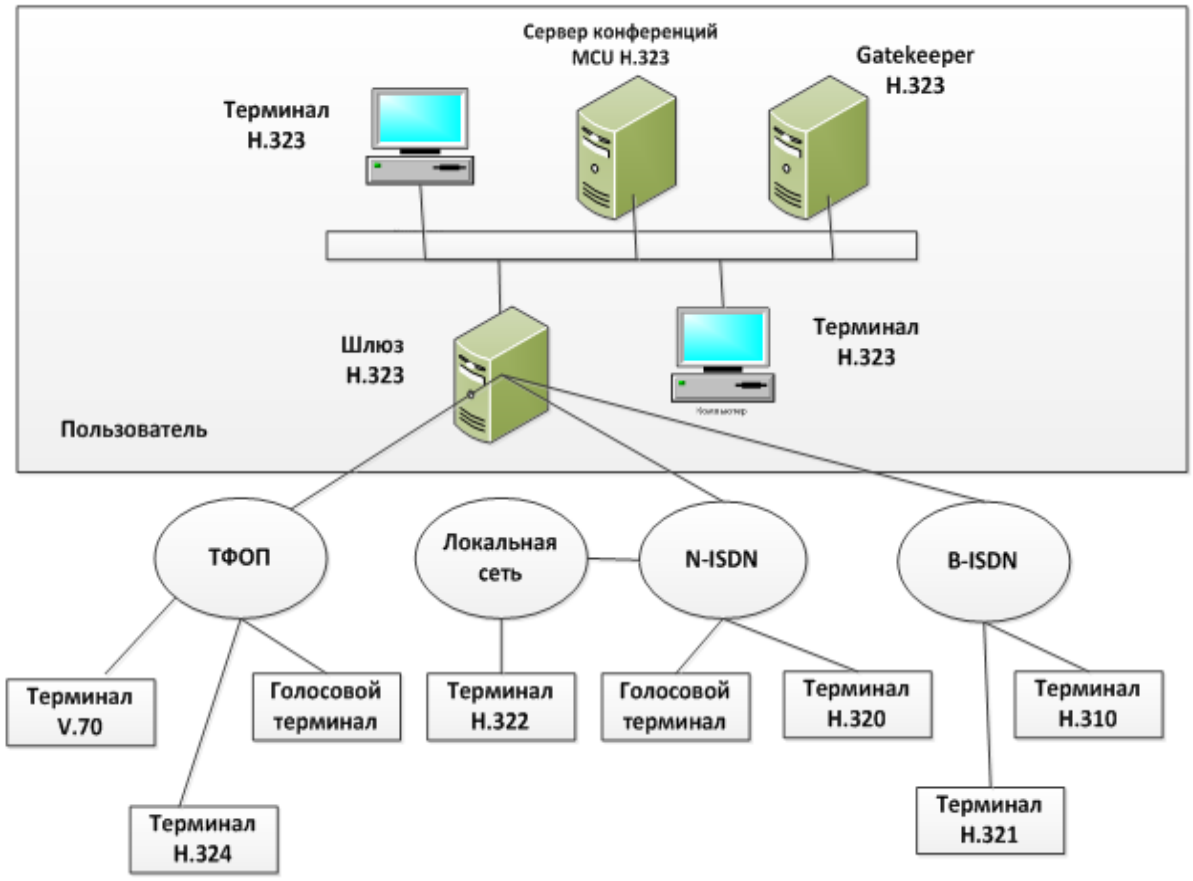


Рисунок 2.1 – Конфігурація мережі на базі стандарту H.323

Таблиця 2.1 – 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

Термінали H.323 можуть бути інтегровані у персональні комп'ютери або реалізовані як автономні пристрої. У рекомендації H.323 описуються чотири основні компоненти (рис.2.2):

- термінал;
- gatekeeper (контролер зони);
- шлюз;
- пристрій управління багатоточковою конференцією (MCU).

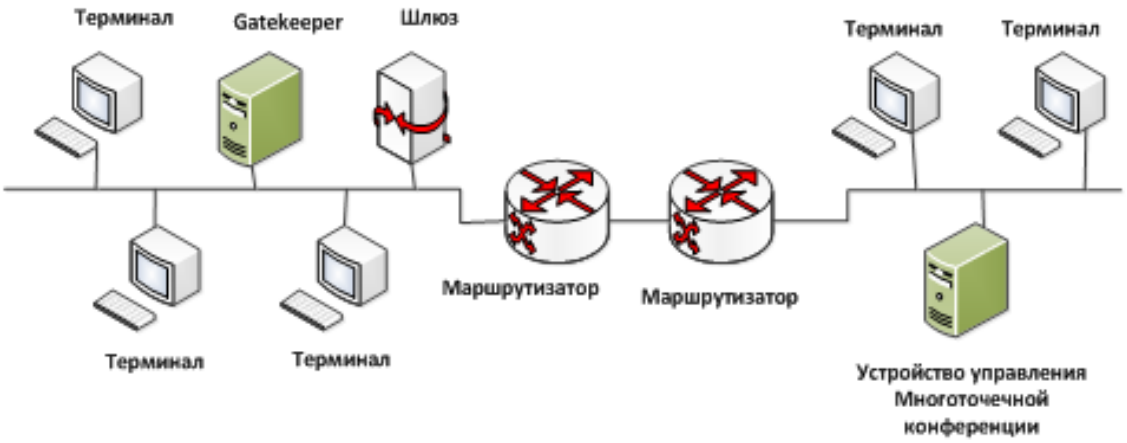


Рисунок 2.2 – Зона H.323

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.

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

Шлюз забезпечує стиснення інформації (голосу), конвертування її (його) в IP-пакети та направлення в IP-мережу. З протилежного боку шлюз здійснює зворотні дії: розшифровку та розформування пакетів викликів. В результаті звичайні телефонні апарати без проблем приймають ці виклики.

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*.

Gatekeeper (контролер зони) – виконує функцію управління викликами. 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 зонами.

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.3. Незалежно від способу апаратної реалізації шлюзи IP-телефонії можуть мати ряд характеристик, які приведені нижче.

Рисунок 2.3 – 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 характеристикою 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.

2.3 Архітектура системи на базі проекту TIPHON

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.

MG виконує наступні задачі: перетворення і/або перекодування передаваємої інформації; трансляція адрес; ехоподавлення; відтворення різних повідомлень для абонентів; прийом та передавання цифр. Основна функція MG – перетворення ІКМ-трафіку у IP-пакети і навпаки.

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.2.4.

Рисунок 2.4 – Функціональна архітектура, яка запропонована в межах проекту TIPHON

Контрольні запитання для самооцінки рівня знань

1. Які основні компоненти стандарту H.323?
2. Які функції виконує gatekeeper (контролер зони) в IP-мережі?
3. Яким чином класифікуються шлюзи IP-телефонії?
4. Які компоненти має функціональна модель TIPHON?
5. На які функціональні об’єкти розділений шлюз IP-телефонії?

3 ПРОЕКТ ПРОТОКОЛУ SIP

3.1 Принципи протоколу SIP

Протокол ініціювання сеансів SIP (англ. Session Initiation Protocol) – є протоколом прикладного рівня і призначений для організації, модифікації та завершення сеансів зв’язку: мультимедійних конференцій, телефонних з’єднань та розподілу мультимедійної інформації. Користувачі можуть приймати участь у існуючих сеансах зв’язку, запрошувати інших користувачів та бути запрошеними ними до нового сеансу зв’язку. Запрошення можуть бути адресовані визначеному

користувачу, групі користувачів або всім користувачам [4].

Протокол SIP розроблений групою MMUSIC (Multiparty Multimedia Session Control) комітету IETF (Internet Engineering Task Force), а специфікації протоколу представлені в документі RFC 2543.

Протокол встановлення сеансу SIP – пропонований стандарт на спосіб установки, зміни і завершення сеансу користувача, що включає мультимедійні елементи, такі як відео або голос, миттєві повідомлення (instant messaging), он-лайн ігри та віртуальну реальність. SIP – стандарт на спосіб встановлення та завершення інтернет-сеансу користувача, який включає обмін мультимедійним вмістом (відео- та аудіоконференція, миттєві повідомлення, он-лайн-ігри).

В моделі взаємодії відкритих систем SIP є мережним протоколом прикладного рівня.

Протокол почав розроблятися у 1996 році Хенінгом Шулзрі (Колумбійський університет) і Марком Хендлі (Університетський коледж Лондона). У листопаді 2000 року SIP був затверджений як сигнальний протокол проекту 3GPP і основний протокол архітектури IMS (модифікація 3GPP TS.24.229). Разом з протоколом H.323, SIP – один з протоколів, що лежать в основі Voice over IP.

Протокол SIP є лише одним із протоколів, які забезпечують мультимедійний обмін через мережу Інтернет. SIP представляє собою сигнальний протокол, який дозволяє одному партнеру надіслати запит іншому та узгодити параметри мультимедіа сесії (RFC-2848, -3050, -3261-65, -3311-13, -3319, -3325, -3329, -3351, -3398, -3428, -3455, -3485, -3487, -3515, -3666, -3840, -3891-93, -4123, 4354, -4458, -4497, -4504, -4508, -4538, -4575, -4579, -4596, -4662, -4730, -4740, -4780, -4916, -5002, -5009, -5039, -5049, -5079, -5118). Транспортування мультимедіа даних звичайно здійснюється за допомогою протоколу RTP (Real-Time Transport Protocol).

Протокол SIP описує, яким чином прикладення клієнта (наприклад, софтфон) може отримати запит початку з’єднання у іншого, можливо, фізично віддаленого клієнту, що знаходиться у тій самій мережі, використовуючи його унікальне ім’я. Протокол визначає спосіб узгодження між клієнтами про відкриття каналів

обміну на основі інших протоколів, які можуть використовуватися для безпосереднього передавання інформації (наприклад, RTP). Допускається добавлення або вилучення таких каналів протягом встановленого сеансу, а також підключення та виключення додаткових клієнтів (тобто допускається участь в обміні більше, ніж двом сторонам – конференц-зв'язок). Протокол також визначає порядок завершення сеансу.

В основу протоколу робоча група MMUSIC заклала наступні принципи:

- *Простота.* Включає тільки шість методів (функцій).
- *Незалежність від транспортного рівня*, може використовувати UDP, TCP, ATM і т.д.
- *Економічність*. Всі запити формуються на основі тексту.
- *Персональна мобільність користувачів*. Користувачі можуть переміщуватися в межах мережі без обмежень, тому послуги зв’язку повинні надаватися їм в будь-якому місці цієї мережі. Це досягається шляхом присвоєння користувачу унікального ідентифікатора, а мережа надає йому послуги зв’язку не залежно від того, де він знаходиться (набір послуг, які надаються, залишається незмінним). Для цього користувач за допомогою спеціального повідомлення – REGISTER – інформує про свої переміщення сервер визначення місцеположення.
- *Масштабність мережі*. Структура мережі на базі протоколу SIP дозволяє легко її розширювати та збільшувати кількість елементів. Серверна структура мережі, яка побудована на основі протоколу SIP, у повному обсязі відповідає цій вимозі.
- *Розширюваність протоколу*. Протокол характеризується можливістю доповнювати його новими функціями при появі нових послуг та його адаптацією до роботи з різними прикладеннями. В якості прикладу можна привести ситуацію, коли протокол SIP використовується для встановлення з’єднання між шлюзами, що взаємодіють з ТфЗК за допомогою сигналізації ЗКС-7 або DSS1. На теперішній час SIP не підтримує «прозоре» передавання сигнальної інформації телефонних систем сигналізації. Внаслідок цього додаткові послуги ISDN є недоступними для користувачів IP мереж. Розширення функцій протоколу SIP

може бути виконане за рахунок нових заголовків повідомлень, які повинні бути зареєстровані в організації IANA. При цьому, якщо SIP сервер приймає повідомлення з невідомими йому полями, він просто ігнорує їх і обробляє лише ті поля, які знає. Для розширення можливостей протоколу SIP можуть бути також добавлені і нові типи повідомлень.

- *Інтеграція в стек існуючих протоколів Інтернет.* Протокол SIP є частиною глобальної архітектури мультимедіа, яка розроблена комітетом IETF. Крім SIP, ця архітектура включає в себе протокол резервування ресурсів (Resource Reservation Protocol - RSVP, RFC 2205), транспортний протокол реального часу (Real Time Transport Protocol - RTP, RFC 1889), протокол передавання потокової інформації у реальному часі (Real Time Streaming Protocol - RTSP, RFC 2326), протокол описання параметрів зв'язку (Session Description Protocol – SDP, RFC 2327). Але функції протоколу SIP не залежать від жодного з цих протоколів.

- *Взаємодія з іншими протоколами сигналізації.* Протокол SIPможе бути використаний разом з протоколом H.323. Можлива також взаємодія протоколу SIP з системами сигналізації ТфЗК – DSS1 та ЗКС-7. Для спрощення такої взаємодії сигнальні повідомлення протоколу SIP можуть переносити не тільки специфічну SIP адресу, але й телефонний номер формату E.164 або будь-якого іншого формату. Крім того, протокол SIP разом з протоколами H.323 та ISUP/IP може застосовуватися для синхронізації роботи пристроїв управління шлюзами; в цьому випадку він повинен взаємодіяти з протоколом MGCP. Іншою важливою особливістю протоколу SIP є те, що він пристосований до організації доступу користувачів мереж IP телефонії до послуг інтелектуальних мереж, і є припущення, що саме цей протокол стане основним при організації зв'язку між вказаними мережами.

3.2 Дизайн протоколу SIP

Клієнти SIP традиційно використовують порт 5060 TCP і UDP для з'єднання серверів та інших елементів SIP-мережі. В основному SIP використовується для встановлення і роз'єднання голосових і відеодзвінків. При цьому він може

використовуватися і в будь-яких інших прикладеннях, де потрібне встановлення з’єднання таких, як системи повідомлення, мобільні термінали і т.д. Існує велика кількість рекомендацій RFC, що відносяться до SIP і визначають поведінку таких прикладень. Для передавання самих голосових і відеоданих використовують інші транспортні протоколи, найчастіше Real-time Transport Protocol (RTP).

Головним завданням розробки SIP було створення сигнального протоколу і протоколу встановлення з’єднань на базі IP, який міг би підтримувати розширений набір функцій обробки виклику та послуг, представлених в існуючій ТфЗК. Сам протокол SIP не визначає цих функцій, а зосереджений тільки на процедурах встановлення дзвінків та сигналізації. При цьому він був спроектований з підтримкою таких функціональних елементів мережі, як проксі-сервери (Proxy Servers) та агенти користувачів (User Agents). Ці елементи забезпечують базовий набір послуг: набір номеру, дзвінок телефонного апарату, можливість після набору почути довгі або короткі гудки, тобто звукове інформування абонента про статус виклику.

Телефонні мережі на базі SIP можуть підтримувати і більш сучасні послуги, що зазвичай надаються ЗКС-7, не дивлячись на значну відмінність цих двох протоколів. ЗКС-7 характеризується складною, централізованою інтелектуальною мережею і простими, неінтелектуальними терміналами (традиційні телефонні апарати). SIP є протоколом типу «точка-точка». Як протоколи такого класу він вимагає тільки дуже просту (і, відповідно, добре масштабовану) мережу з інтелектом, вбудованим у кінцеві елементи на периферії (термінали, побудовані як фізичні пристрої або програми). Іншими словами, функції SIP реалізовані в термінальних пристроях (тобто на межі мережі), на відміну від традиційних можливостей ЗКС-7, які підтримуються самою мережею.

Хоча існує багато інших сигнальних протоколів VoIP, SIP характеризується його прихильниками як такий, який належить до співтовариства IP, а не до телекомунікаційної індустрії. SIP стандартизований і контролюється головним чином IETF, тоді як протокол H.323 сімейства VoIP був традиційно тісніше пов'язаний з ITU. Проте ці дві організації так чи інакше схвалили обидва

протоколи.

SIP використовується разом з декількома іншими протоколами і бере участь тільки в сигнальній частині сесії (сеансу) зв'язку. SIP виконує роль носія для SDP, який описує параметри передавання медіаданих в межах сесії, наприклад, порти IP, які використовуються та кодеки. У типовому застосуванні «сесії» SIP – це просто потоки пакетів RTP. RTP є безпосереднім носієм голосових даних і відеоданих.

Перша запропонована версія стандарту (SIP 2.0) була визначена у RFC 2543. Протокол був додатково уточнений у RFC 3261, хоча багато реалізацій як і раніше основано на проміжних версіях стандарту. Номер версії протоколу SIP і залишився 2.0.

SIP схожий на HTTP і розділяє з ним загальні принципи проектування: він придатний для читання людиною і структурований відносно запитів і відгуків. Прихильники SIP також заявляють про нього як про простіший, у порівнянні з H.323. Проте, деякі схильні вважати, що тоді як спочатку метою SIP була простота, у своєму сьогоднішньому вигляді він став так само складним, як і H.323. Інші вважають, що SIP – протокол без станів, який тим самим дає легко реалізувати відновлення при відмові і інші можливості, які ускладнені в протоколах із станами, таких як H.323. SIP розділяє з HTTP багато кодів станів, таких як відомий '404 not found'. SIP та H.323 не обмежені голосовим зв'язком, вони можуть обслуговувати будь-який сеанс зв'язку, від голосового до відеосеансу або майбутні види зв'язку.

3.3 Архітектура SIP мережі

Протокол SIP має клієнт-серверну архітектуру (рис.3.1).

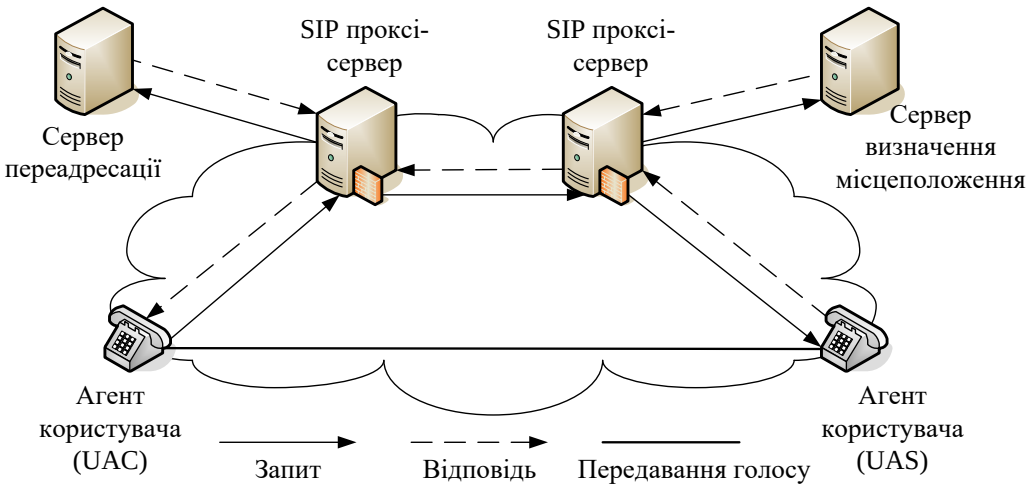


Рисунок 3.1 - Архітектура протоколу SIP

Клієнт є суб'єктом мережі, який надсилає SIP-запити і отримує SIP-відповіді. Клієнти, якщо це необхідно, можуть безпосередньо взаємодіяти з людиною. Агент користувача клієнта і проксі є клієнтами.

Сервер є елементом мережі, який отримує запити і який повинен їх обслуговувати, надсилаючи відповіді. Прикладами серверів є проксі, агенти користувача серверів, сервери переадресації та регістратори.

Клієнт видає запити, із вказуванням того, що він хоче отримати від сервера. Сервер приймає та обробляє запити, видає відповіді, що містять повідомлення про успішність виконання запиту, повідомлення про помилку або інформацію, яка запитується клієнтом.

Управління процесом обслуговування виклику розподілене між різними елементами мережі SIP. Основним функціональним елементом, який реалізує функції управління з'єднанням, є термінал. Інші елементи мережі відповідають за маршрутизацію викликів, а в деяких випадках надають додаткові послуги.

Термінал. Коли клієнт і сервер реалізовані у кінцевому обладнанні і взаємодіють безпосередньо з користувачем, вони називаються *агентським клієнтом користувача* - User Agent Client (UAC) і *агентським сервером користувача* - User Agent Server (UAS). Якщо у пристрої є UAC і UAS, пристрій називається *агентом користувача* - User Agent (UA) і представляє собою термінальне обладнання SIP.

Сервер UAS і клієнт UAC мають можливість безпосередньо взаємодіяти з

користувачем. Інші клієнти і сервери SIP цього робити не можуть.

Крім терміналів, визначені два основних типи елементів мережі SIP: проксі-сервер (proxy server) і сервер переадресації (redirect server).

Проксі-сервер. Проксі-сервер (від англ. proxy – «представник») представляє інтереси користувача в мережі. Він приймає запити, обробляє їх і виконує відповідні дії. Це може бути пошук і виклик користувача, маршрутизація запиту, надавання послуг і т.д. Проксі-сервер складається з клієнтської та серверної частин, тому може приймати виклики, ініціювати власні запити та повертати відповіді. Проксі-сервер може бути фізично поєднаний із сервером визначення місцеположення (в цьому випадку він називається registrar) або існувати окремо від цього сервера, але мати можливість взаємодіяти з ним по протоколам LDAP (RFC 2167) або по будь-яким іншим протоколам.

Передбачено два види проксі-серверів:

- із зберіганням станів (stateful). Такий сервер зберігає у своїй пам’яті всі отримані запити і пов’язані з ним нові сформовані запити до закінчення транзакції.
- без збереження станів (stateless). Такий сервер обробляє отримані запити, але на його основі не можна реалізувати складні, інтелектуальні послуги.

Сервер першого типу дозволяє надавати велику кількість послуг, але працює повільніше, ніж сервер другого типу. Він може застосовуватися для обслуговування невеликої кількості клієнтів, наприклад, у локальній мережі. Проксі-сервер повинен зберігати інформацію про стани, якщо він: використовує протокол TCP для передавання сигнальної інформації; працює в режимі багатоадресної розсилки сигнальної інформації; розмножує запити.

Останній випадок має місце, коли проксі-сервер здійснює пошук викликаємого користувача зразу в декількох напрямках, тобто один запит, який надійшов до проксі-сервера, розмножується і передається одночасно за всіма цими напрямками.

Сервер без збереження станів просто ретранслює запити та відповіді, які отримує. Він працює швидше, ніж сервер першого типу, так як ресурс процесора

не витрачається на запам’ятовування станів, внаслідок чого сервер цього типу може обслуговувати велику кількість користувачів. Недоліком такого сервера є те, що на його основі можна реалізувати лише найбільш прості послуги. Проксі-сервер може функціонувати як сервер із збереженням станів для одних користувачів і як сервер без збереження станів – для інших.

Алгоритм роботи користувачів з проксі-сервером має наступний вигляд. Постачальник послуг IP-телефонії повідомляє адресу проксі-сервера своїм користувачам. Викликаючий користувач передає до проксі-сервера запит з’єднання. Сервер обробляє запит, визначає місцеположення викликаємого користувача і передає запит цьому користувачу, а потім отримує від нього відповідь, яка підтверджує успішну обробку запиту, і транслює цю відповідь користувачу, який передав запит. Проксі-сервер може модифікувати деякі заголовки повідомлень, які він транслює, причому кожний сервер, який обробив запит в процесі його передавання від джерела до приймача, повинен вказати це у SIP-запиті для того, щоб відповідь на запит повернулася тим же шляхом.

Сервер переадресації. Сервер переадресації використовується для визначення поточної адреси, тобто поточного місцеположення користувача. Викликаючий користувач передає до сервера повідомлення з відомою йому адресою викликаємого користувача, а сервер забезпечує переадресацію виклику на поточну адресу цього користувача. Для реалізації цієї функції сервер пере-адресації повинен взаємодіяти із сервером визначення місцеположення. Серевер переадресації не термінує виклики і не ініціює власні запити, а тільки повідомляє адресу необхідного терміналу або проксі-сервера. За цією адресою ініціатор запиту передає новий запит. Сервер переадресації не містить клієнтську частину програмного забезпечення. Але користувачу не обв’язково зв’язуватися з будь-яким SIP-сервером. Він може сам викликати іншого користувача за умови, що знає його поточну адресу.

Сервер визначення місцеположення користувачів. Користувач може переміщуватися у межах мережі SIP, тому існує механізм визначення його місцеположення у поточний момент часу. Наприклад, співробітник підприємства

від’їжджає у відрядження і всі виклики, які йому адресовані, повинні бути направлені до іншого міста на його тимчасове місце роботи. Про те, де він знаходиться, користувач інформує спеціальний сервер за допомогою повідомлення REGISTER. Можливі два режими реєстрації: користувач може повідомити свою нову адресу один раз, а може реєструватися періодично через визначені проміжки часу. Перший спосіб підходить для випадку, коли термінал, який доступний користувачу, включений постійно і його не переміщують по мережі, а другий – коли термінал часто переміщується або виключається.

Сервер визначення місцеположення користувачів необхідний для зберігання поточної адреси користувача і представляє собою базу даних адресної інформації. Крім постійної адреси користувача, у цій базі даних може зберігатися одна або декілька поточних адрес. Цей сервер може бути сполучений з проксі-сервером (у такому випадку він називається registar) або бути реалізованим окремо від проксі-сервера, але мати можливість зв’язуватися з ним.

У RFC 2543 сервер визначення місцеположення представлений як окремий елемент мережі, але принципи його роботи в цьому документі не регламентовані. Необхідно звернути увагу на те, що викликаючий користувач, якому потрібна поточна адресна викликаємого користувача, не зв’язується із сервером визначення місцеположення напряму. Цю функцію виконують інші SIP-сервери за допомогою протоколів LDAP (RFC 1777), rwhois (RFC 2167) та інших протоколів.

Ресурси у конфігурації SIP ідентифікуються URI. Прикладами ресурсів можуть бути:

- обмін даними у реальному масштабі часу;
- поява багатоканального телефонного виклику;
- поштова скринька системи обміну повідомленнями;
- телефонний номер послуг шлюзу;
- група (така як «група продажу» або «група підтримки») в організації.

SIP-телефони – це те саме, що й VoIP-телефони або програмні телефони. Це телефони, які дозволяють здійснювати телефонні виклики з використанням технології VoIP (голос, який передається по інтернет-протоколу).

Існують два типи SIP-телефонів. Перший – це апаратний SIP-телефон, який нагадує звичайний телефон, але приймає та здійснює виклики по мережі Інтернет замість звичайної системи ТфЗК. SIP-телефони також можуть бути реалізовані програмно. Це дозволяє використовувати в якості телефону будь-який комп'ютер, скориставшись телефонною гарнітурою та мікрофоном і/або звуковою картою. Необхідні також провайдер VoIP та SIP-сервер.

Телефонна система *3CX* для Windows може використовуватися з найбільш популярними апаратними SIP-телефонами. Система також має безкоштовний програмний SIP-телефон, який функціонує як VoIP-клієнт для телефонної системи *3CX*.

3.4 Адресація протоколу SIP

Для організації взаємодії з існуючими прикладеннями IP-мереж і для забезпечення мобільності користувачів SIP використовує адресу електронної пошти. В якості адрес робочих станцій використовуються універсальні вказівники ресурсів URL (Universal Resource Locators), так називаємі SIP URL. SIP-адреси бувають чотирьох типів:

ім'я@домен,

ім'я@хост,

ім'я@IP-адреса,

№телефону@шлюз.

Таким чином, адреса складається з двох частин. Перша частина – це ім'я користувача, який зареєстрований в домені або на робочій станції. Якщо друга частина ідентифікує будь-який шлюз, то в першій вказується телефонний номер абонента. У другій частині адреси вказується ім'я домену, робочої станції або шлюзу. Для визначення IP-адреси пристрою необхідно звернутися до служби доменних імен – Domain Name Service (DNS). Якщо ж у другій частині SIP-адреси розміщується IP-адреса, то з робочою станцією можна зв'язатися напряму.

На початку SIP-адреси (в тексті) ставиться слово sip:, яке вказує що це саме SIP-адреса, оскільки бувають і інші з таким же форматом (наприклад, адреси

електронної пошти, які позначаються mailto:). Приклади SIP-адрес:

sip: als@rts.loniis.ua

sip: user1@192.168.100.152

sip: 294-75-47@gateway.ua

Імена користувачів представляють собою звичайні алфавітно-цифрові ідентифікатори [9]. В IP-телефонії, як правило, використовують лише цифрові ідентифікатори («номери») для зручності розширення/заміни класичних телефонних мереж. Номери місцевого зв'язку, як правило, 2-3-4 – значні.

Номер телефону, що передається шлюзу – будь-який доступний через нього, і може бути як номером місцевого зв'язку, так і номером мобільного або звичайного міського телефону. Адреса шлюзу (IP-адреса або ім'я домену) задається в налаштуваннях телефону або програми-клієнта, а користувачу для здійснення дзвінка достатньо тільки набору номера.

3.5 Інтеграція SIP з IP мережами

Однією з важливих особливостей протоколу SIP є його незалежність від транспортних технологій. В якості транспорту можуть використовуватися протоколи X.25, Frame Relay, AAL5/ATM, IPX та інші. Структура повідомлень SIP не залежить від вибраної транспортної технології. Але, в той же час, перевага надається технології маршрутизації пакетів IP та протоколу UDP. При цьому необхідно створити додаткові механізми для надійної доставки сигнальної інформації. До таких механізмів відноситься повторне передавання інформації при її втраті, підтвердження прийому та ін.

Сигнальні повідомлення можуть переноситися не тільки протоколом транспортного рівня UDP, але й протоколом TCP. Протокол UDP дозволяє швидше, ніж TCP, доставляти сигнальну інформацію (навіть з урахуванням повторного передавання непідтверджених повідомлень), а також проводити паралельний пошук місця положення користувачів та передавати запрошення до участі у сеансі зв'язку в режимі багатоадресної розсилки. У свою чергу, протокол TCP спрощує роботу з міжмережними екранами (firewall), а також гарантує

надійну доставку даних. При використанні протоколу TCP різні повідомлення, що відносяться до одного виклику, можуть передаватися по одному TCP-з'єднанню або для кожного запиту та відповіді на нього може відкриватися окреме TCP-з'єднання.

По мережі з маршрутизацією пакетів IP може передаватися інформація практично у будь-якому вигляді: мова, відео та дані, а також будь-яка їх комбінація, що називається мультимедійною інформацією. При організації зв'язку між терміналами користувачів необхідно попередити зустрічну сторону про те, якого роду інформація може прийматися (передаватися), алгоритм її кодування та адреса, на яку необхідно передавати інформацію. Таким чином, однією з обов'язкових умов організації зв'язку за допомогою протоколу SIP є обмін між сторонами даними про їх функціональні можливості. Для цієї мети найчастіше використовується протокол опису сеансів зв'язку – SDP (Session Description Protocol). Оскільки, протягом сеансу зв'язку може відбуватися його модифікація, передбачене передавання повідомлень SIP з новим описом сеансу засобами SDP.

Для передавання мовної інформації комітет IETF пропонує використовувати протокол RTP, але сам протокол SIP не виключає можливості використання для цієї мети інших протоколів.

У протоколі SIP не реалізовані механізми управління потоками інформації та надавання гарантованої якості обслуговування. Крім того, протокол SIP не призначений для передавання інформації користувачів, у його повідомленнях може переноситися інформація тільки в обмеженому обсязі. При перенесенні через мережу дуже великого повідомлення SIP не виключена його фрагментація на рівні IP, що може вплинути на якість передавання інформації.

У глобальній інформаційній мережі Інтернет вже досить давно функціонує експериментальна ділянка Mbone, яка утворена з вузлів мережі, які підтримують режим багатоадресної розсилки мультимедійної інформації. Найважливішою функцією Mbone є підтримка мультимедійних конференцій, а основним способом запрошення учасників до конференції став протокол SIP.

Протокол SIP передбачає організацію конференцій трьох видів:

- у режимі багатоадресної розсилки (multicasting), коли інформація передається на одну multicast-адресу, а потім доставляється мережею кінцевим адресатам;
- за допомогою пристрою управління конференції (MCU), до якого учасники конференції передають інформацію в режимі «точка-точка», а він, у свою чергу, обробляє її (тобто змішує або комутує) та розсилає учасникам конференції;
- шляхом з'єднання кожного користувача у режимі «точка-точка».

Протокол SIP дає можливість приєднання нових учасників до вже існуючого сеансу зв'язку, тобто двосторонній сеанс може перейти у конференцію.

Необхідно відмітити те, що розроблені методи сумісної роботи цього протоколу з перетворювачем мережних адрес – Network Address Translator (NAT).

Для взаємодії з традиційними телефонними мережами, які використовують сигналізацію ЗКС-7, була розроблена модифікація протоколу SIP для телефонії: Session Initiation Protocol for Telephones (SIP-T). Даний протокол описаний в RFC 3372. Основна задача даної модифікації протоколу SIP полягає у «прозорому» передаванні повідомлень ISUP по IP-мережі. Дана задача здійснюється шляхом інкапсуляції сигнальних одиниць ЗКС у повідомлення SIP. Всі необхідні задачі по взаємодії між протоколами були вирішені на базі протоколу SIP (табл.3.1).

Таблиця 3.1 – Взаємодія між протоколами

Вимоги по взаємодії	Функції SIP-T
«Прозорість» сигналізації ISUP.	Інкапсуляція ISUP у тіло повідомлення SIP.
Можливість здійснення маршрутизації повідомлень SIP в залежності від ISUP.	Трансляція параметрів ISUP у заголовку повідомлення SIP.
Трансляція адресної інформації при встановленому з'єднанні.	Використання методу INFO.

У більшості клієнтів SIP шифрування не забезпечується і весь трафік здійснюється у відкритому вигляді. Але є можливість виконати шифрування шляхом тунелювання IP трафіку.

Контрольні запитання для самооцінки рівня знань

1. У чому полягало основне завдання розробки протоколу SIP?
2. Призначення та функції протоколу SIP?
3. На якому рівні моделі OSI використовується протокол SIP?
4. Які принципи покладені в основу протоколу SIP?
5. Яким чином здійснюється розширення функцій протоколу SIP?
6. Яким чином відбувається взаємодія SIP з іншими протоколами сигналізації?
7. Яку архітектуру має протокол SIP?
8. Які функції виконує проксі-сервер? Види проксі-серверів?
9. У чому полягає алгоритм роботи користувачів з проксі-сервером?
10. Які ресурси використовуються у конфігурації SIP?

4 АЛГОРИТМИ ВСТАНОВЛЕННЯ SIP З'ЄДНАННЯ

4.1 Повідомлення протоколу SIP. Структура повідомлень SIP

Згідно архітектурі «клієнт-сервер» всі повідомлення поділяються на запити, які передаються від клієнта до сервера, та на відповіді сервера клієнту. Наприклад, щоб ініціювати встановлення з'єднання, викликаючий користувач повинен повідомити серверу ряд параметрів, у тому числі, адресу викликаємого користувача, параметри інформаційних каналів та ін. Ці параметри передаються у спеціальному SIP-запиті. Від викликаємого користувача до викликаючого передається відповідь на запит, яка також містить ряд параметрів.

Всі повідомлення протоколу SIP (запити та відповіді) представляють собою послідовності текстових рядків, які закодовані у відповідності з документом RFC 2279. Структура та синтаксис повідомлень SIP ідентичні тим, які використовуються в протоколі HTTP. Структура повідомлень протоколу SIP приведена на рис.4.1.

Рисунок 4.1 - Структура повідомлень протоколу SIP

Стартовий рядок – початковий рядок будь-якого SIP – повідомлення. Якщо повідомлення є запитом, у ньому вказується тип запиту, адресат та номер версії протоколу. Якщо повідомлення є відповіддю на запит, у ньому вказується номер версії протоколу, тип відповіді та його коротке розшифрування, призначене тільки для користувача.

Заголовки повідомлень містять інформацію, яка необхідна для обробки повідомлення (інформація про передавача, адресата, шляхи прямування і т.д.). Про тип заголовка можна дізнатися за його ім’ям. Воно не залежить від регістру (тобто літери можуть бути прописними та рядковими), але звичайно ім’я пишуть з великої літери, за якою йдуть рядкові.

Тіло повідомлення містить опис сеансів зв’язку, наприклад, у запитах ACK, INIVITE та OPTIONS. Не всі запити містять тіло повідомлення (наприклад, запит BYE). Всі відповіді можуть містити тіло повідомлення, але вміст тіла в них буває різним. Приклад запиту INVITE:

INVITE sip:nikolia@zenit.chempion.spb.ua SIP/2.0

Record-Route: sip:nikolia@10.0.0.10;lr

Via: SIP/2.0/UDP 10.0.0.10;branch=z9hG4bK3af7.0a6e92f4.0

Via: SIP/2.0/UDP 192.168.0.2:5060;branch=z9hG4bK12ee92cb;rport=5060

From: “78128210000” sip:78128210000@vladimir.spb.ua;tag=as149b2d97

To: <sip:nikolia@zenit.chempion.spb.ua>

Contact: < sip:78128210000@vladimir.spb.ua >

Call-ID: 3cbf958e6f43d91905c3fa964a373dcb_ zenit.chempion.spb.ua

CSeq: 103 INVITE

Max-Forwards: 16

Date: Wed, 10 Jan 2001 13:16:23 GMT

Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY

Supported: replaces

Content-Type: application/sdp

Content-Length:394

v=0

o=root 3303 3304 IN IP4 10.0.0.10

s=session

c=IN IP4 10.0.0.10

t=0 0

m=audio 40358 RTP/AVP 0 8 101

a=rtmap:0 PCMU/8000

a=rtmap:8 PCMU/8000

a=rtmap:101 telephone-event/8000

a=fmtp:101 0-16

a=silenceSupp:off----

a=sendrecv

4.2 Заголовки повідомлень SIP

У протоколі SIP визначено чотири види заголовків (табл.3.1):

- загальні заголовки, які присутні у запитах та відповідях;
- заголовки вмісту, переносять інформацію про розмір тіла повідомлення або про джерело запиту (починаються із слова);
- заголовки запитів, що передають додаткову інформацію про запит;
- заголовки відповідей, що передають додаткову інформацію про відповідь.

Таблиця 4.1 - Види заголовків повідомлень SIP

Загальні заголовки	Заголовки вмісту	Заголовки запитів	Заголовки Відповідей
Call-ID (ідентифікатор сеансу зв’язку)	Content-Encoding (кодування тіла повідомлення)	Accept (приймається)	Allow (дозвіл)
Contact (контактувати)	Content-Length (розмір тіла повідомлення)	Accent-Encoding (метод кодування підтримується)	Proxy-Authenticate (підтвердження справжньості проксі-сервера)
CSeq (послідовність)	Content-Type (тип вмісту)	Accent-Language (мова підтримується)	Retro-After (повторити через деякий час)
Date (дата)		Authorization (авторизація)	Server (сервер)
Encryption (шифрування)			Unsupported (не підтримується)
Expires (спрацювання таймеру)		Hide (сховати)	Warning (попередження)
From (джерело запиту)		Max-Forwards (максимальна кількість переадресацій)	WWW-Authenticate (підтвердження справжності WWW-сервера)
Record-Route (запис маршруту)		Organization (організація)	
Timestamp (мітка часу)		Priority (пріоритет)	

To (адресат)		Proxy-Authorization (авторизація проксі-сервера)	
Via (через)		Proxy-Require (необхідно проксі-сервер)	
		Route (маршрут)	
		Require (необхідно)	
		Response-Key (ключ кодування відповіді)	
		Subject (тема)	
		User-Agent (агент користувача)	

Заголовок містить назву, за якою прямує значення заголовку, відокремлене двома крапками. У полі значення містяться передаваємі дані. Необхідно зазначити, що якщо сервер приймає повідомлення, заголовки яких йому невідомі, ці заголовки ігноруються. Нижче представлені заголовки, які використовуються найчастіше.

Заголовок Call-ID – унікальний ідентифікатор сеансу зв'язку або всіх реєстрацій окремого клієнта, він схожий на мітку з'єднання (call reference) у сигналізації DSS-1. Значення ідентифікатору присвоює сторона, яка ініціює виклик. Заголовок Call-ID складається з буквенно-числового значення та імені робочої станції, яка присвоїла значення цьому ідентифікатору. Між ними повинен знаходитися символ @, наприклад, 2345call@rts.domen.ua. Можлива наступна ситуація: до однієї мультимедійної конференції відносяться декілька з'єднань, тоді всі вони будуть мати різні ідентифікатори Call-ID.

Заголовок To – визначає адресата. Крім SIP-адреси, тут може використовуватися параметр для ідентифікації визначеного терміналу користувача (наприклад, домашнього, робочого або стільникового телефону) у тому випадку, коли всі його термінали зареєстровані під однією адресою SIP URL. Запит може помножуватися та досягти різних терміналів користувача; щоб їх розрізняти, необхідно мати мітку tag. Її вставляє в заголовок термінальне обладнання викликаного користувача при відповіді на прийнятий запит. Якщо потрібне візуальне виведення імені користувача, наприклад, на дисплей, то ім’я користувача також розміщується у полі To.

Заголовок From – ідентифікує відправника запиту; за структурою аналогічний полю To.

Заголовок CSeq – унікальний ідентифікатор запиту, що відноситься до одного з’єднання. Він необхідний для кореляції запиту з відповіддю на нього. Заголовок складається з двох частин: натурального числа з діапазону від 1 до 232 та типу запиту. Сервер повинен перевіряти значення CSeq у кожному запиті, який приймається, і вважати запит новим, якщо значення CSeq більше, ніж попереднє. Приклад заголовку: CSeq: 2 INVITE.

Заголовок Via необхідний для того, щоб запобігти ситуації, коли запит надійде до замкнутого кола, а також для тих випадків, коли необхідно, щоб запити обов’язково проходили по одному і тому ж шляху (наприклад, у випадку використання міжмережного екрану – firewall). Справа в тому, що запит може проходити через декілька проксі-серверів, кожний з яких приймає, обробляє та перенаправляє запит до наступного проксі-сервера, і так до тих пір, поки запит не надійде до адресата. Таким чином, у заголовку Via вказується весь шлях, пройдений запитом: кожний проксі-сервер добавляє поле із своєю адресою. За необхідністю (наприклад, щоб забезпечити секретність) дійсна адреса може приховуватися [7].

Наприклад, запит на своєму шляху обробляється двома проксі-серверами: спочатку сервером domen.ru, потім sip.telecom.com. Тоді у запиті з’являються наступні поля:

Via: SIP/2.0/UDP sip.telecom.com:5060;branch=721 e418c.4.1

Via: SIP/2.0/UDP domen.ru: 5060,

де параметр означає, що на сервері sip.telecom.com запит був розмножений та направлений одночасно по різним напрямкам, і наш запит був переданий за напрямком, який ідентифікується наступним чином: 721e418c.4.1.

Вміст полів Via копіюється із запитів на відповіді на них і кожний сервер, через який проходить відповідь, видаляє поле Via із своїм ім'ям.

У заголовок Record-route проксі-сервер вписує свою адресу – SIP URL, - якщо треба, щоб наступні запити пройшли через нього.

Заголовок Content-Type визначає формат опису сеансу зв'язку. Сам опис сеансу, наприклад, у форматі протоколу SDP, включається в тіло повідомлення.

Заголовок Content-Length вказує розмір тіла повідомлення.

Після того, як ми розглянули заголовки протоколу SIP, які найчастіше зустрічаються, необхідно звернути увагу на те, що запити та відповіді на них можуть включати в себе лише визначений набір заголовків (табл.4.2). Літера F означає обов'язкову присутність заголовка у повідомленні, літера M – необов'язкову присутність, літера O забороняє присутність заголовку.

Таблиця 4.2 - Зв'язок заголовків із запитами та відповідями протоколу SIPv2.0

Назва заголовку	Місце використання Заголовку	ACK	BYE	CAN	INV	OPT	REG
Accept	Заголовок у запитах	F	F	F	0	0	0
Accept	Заголовок у відповіді 415	F	F	F	0	0	0
Accent-Encoding	Заголовок у запитах	F	F	F	0	0	0
Accent-Encoding	Заголовок у відповіді 415	F	F	F	0	0	0
Accent-Language	Заголовок у запитах	F	0	0	0	0	0
Accent-Language	Заголовок у відповіді 415	F	0	0	0	0	0
Allow	Заголовок у відповіді 200	F	F	F	F	M	F
Allow	Заголовок у відповіді 405	0	0	0	0	0	0

Authorization	Заголовок у запитах	0	0	0	0	0	0
Call-ID	Загальний заголовок-копіюється із запитів у відповіді	M	M	M	M	M	M
Contact	Заголовок у запитах	0	F	F	0	0	0
Contact	Заголовок у відповідях1xx	F	F	F	0	0	F
Contact	Заголовок у відповідях2xx	F	F	F	0	0	0
Contact	Заголовок у відповідях3xx	F	0	F	0	0	0
Contact	Заголовок у відповіді 485	F	0	F	0	0	0
Content-Encoding	Заголовки вмісту	0	F	F	0	0	0
Content-Length	Заголовки вмісту	0	F	F	0	0	0
Content-Type	Заголовки вмісту	*	F	F	*	*	*
Cseq	Загальний заголовок-копіюється із запитів у відповіді	M	M	M	M	M	M
Date	Заголовок у відповідях	0	0	0	0	0	0
Encryption	Заголовок у відповідях	0	0	0	0	0	0
Expires	Заголовок у відповідях	F	F	F	0	F	0
From	Загальний заголовок-копіюється із запитів у відповіді	M	M	M	M	M	M
Hide	Заголовок у запитах	0	0	0	0	0	0
Max-Forwards	Заголовок у запитах	0	0	0	0	0	0
Organization	Загальний заголовок	F	F	F	0	0	0
Proxy-	Заголовок у відповіді 407	0	0	0	0	0	0

Authenticate							
Proxy-Authorization	Заголовок у запитах	0	0	0	0	0	0
Proxy-Require	Заголовок у запитах	0	0	0	0	0	0
Priority	Заголовок у запитах	F	F	F	0	F	F
Require	Заголовок у запитах	0	0	0	0	0	0
Retry-After	Заголовок у запитах	F	F	F	M	F	0
Retry-After	Заголовок у відповідях 404,480,486,503,600,603	0	0	0	0	0	0
Response-Key	Заголовок у запитах	F	0	0	0	0	0
Record-Route	Заголовок у запитах	0	0	0	0	0	0
Record-Route	Заголовок у відповідях 2xx	0	0	0	0	0	0
Route	Заголовок у запитах	0	0	0	0	0	0
Server	Заголовок у відповідях	0	0	0	0	0	0
Subject	Заголовок у запитах	F	F	F	0	F	F
Timestamp	Загальний заголовок	0	0	0	0	0	0
To	Загальний заголовок-копіюється із запитів у відповіді	M	M	M	M	M	M
Unsupported	Заголовок у відповіді 420	0	0	0	0	0	0
User-Agent	Загальний заголовок	0	0	0	0	0	0
Via	Загальний заголовок-копіюється із запитів у відповіді	M	M	M	M	M	M
Warning	Заголовок у відповідях	0	0	0	0	0	0
WWW-Authenticate	Заголовок у відповіді 401	0	0	0	0	0	0

Поля необхідні тільки в тому випадку, коли тіло повідомлення містить будь-яку інформацію, тобто не є пустим.

4.3 Запити. Відповіді на запити

У теперішній версії протоколу SIP (RFC 3261) визначено шість типів запитів. Кожний з них призначений для виконання досить широкого кола задач, що є суттєвою перевагою протоколу SIP, так як завдяки цьому кількість повідомлень, якими обмінюються термінали та сервери, зведена до мінімуму. За допомогою запитів клієнт повідомляє про поточне місцеположення, запрошує користувачів взяти участь у сеансах зв'язку, модифікує вже встановлені сеанси, закінчує їх і т.д. Сервер визначає тип прийнятого запиту за назвою, яка вказана у стартовому рядку. У тому ж рядку в полі Request-URI вказана SIP-адреса обладнання, якому цей запит адресований. Вміст полів To та Request-URI може відрізнятися, наприклад, у полі To може бути вказана публікуєма адреса абонента, а у полі Request-URI – поточна адреса користувача.

Запит INVITE – запрошує користувача взяти участь у сеансі зв'язку. В основному містить SDP – опис сеансу зв'язку, в якому вказується вид приймаємої інформації та параметри (список можливих варіантів параметрів), які необхідні для прийому інформації, а також може вказуватися вид інформації, яку викликаємий користувач може передавати. У відповіді на запит типу INVITE вказується вид інформації, яка буде прийматися викликаємим користувачем, і, крім того, може вказуватися вид інформації, яку викликаємий користувач збирається передавати (можливі параметри передавання інформації). У цьому повідомленні можуть міститися також дані, які необхідні для аутентифікації абонента і, виходячи з цього, доступи клієнтів до SIP-сервера. За необхідністю змінити характеристики вже організованих каналів передається запит INVITE з новим описом сеансу зв'язку. Для запрошення нового учасника до вже встановленого з'єднання також використовується повідомлення INVITE.

Запит ACK – підтверджує прийом відповіді на запит INVITE. Запит ACK використовується тільки разом із запитом INVITE, тобто цим повідомленням

обладнання викликаючого користувача показує, що отримало кінцеву відповідь на свій запит INVITE. У повідомленні АСК може міститися кінцевий опис сеансу зв'язку, який передається викликаючим користувачам.

Запитом BYE – обладнання викликаємого або викликаючого абонента завершує сеанс зв'язку. Може бути переданий будь-якою із сторін, які приймають участь у сеансі. Сторона, яка отримала запит BYE, повинна завершити передавання мовної (мультимедійної) інформації та підтвердити його виконання відповіддю 200 ОК.

Запит CANCEL – відміняє обробку запитів, які передані раніше, але не впливає на запити, які вже закінчили оброблюватися. Наприклад, запит CANCEL застосовується тоді, коли проксі-сервер розмножує запити для пошуку користувача по декільком напрямкам і в одному з них його не знаходить. Обробку запитів, які розіслані у всі інші напрямки, сервер відміняє за допомогою повідомлення CANCEL.

Запит REGISTER – переносить адресну інформацію для реєстрації користувача на сервері визначення місцеположення, тобто за допомогою запиту типу REGISTER користувач повідомляє своє поточне місцеположення. У цьому повідомленні містяться наступні поля:

- поле To містить адресну інформацію, яку необхідно зберегти або модифікувати на сервері;
- поле From містить адресу ініціатора реєстрації. Зареєструвати користувача може або він сам, або інша особа, наприклад, секретар може зареєструвати свого начальника;
- поле Contact містить нову адресу користувача, за якою повинні передаватися всі подальші запити INVITE. Якщо у запиті REGISTER поле Contact відсутнє, реєстрація залишається попередньою. У випадку відміни реєстрації тут розміщується символ «*»;
- у полі Expires вказується час у секундах, протягом якого реєстрація дійсна.

Якщо дане поле відсутнє, по умовчанню призначається час – 1 година, після чого реєстрація відміняється. Реєстрацію можна також відмінити, передавши

повідомлення REGISTER з полем Expires, якому присвоєно значення О, та з відповідним полем Contact.

Запитом OPTION – викликаємий користувач виконує запит інформації про функціональні можливості термінального обладнання викликаємого користувача. У відповідь на цей запит обладнання викликаємого користувача повідомляє необхідні відомості. Застосування запиту OPTION обмежене тими випадками, коли необхідно дізнатися про функціональні можливості обладнання до встановлення з'єднання. Для встановлення з'єднання запит цього типу не використовується.

Але в процесі розвитку, у протокол було добавлено ще декілька типів запитів, які доповнили його функціональність:

PRACK – тимчасове підтвердження (RFC 3262);

SUBSCRIBE – підписування на отримання повідомлень про подію (RFC 3265);

NOTIFY – повідомлення підписчика про подію (RFC 3265);

PUBLISH – публікування події на сервері (RFC 3903);

INFO – передавання інформації, яка не змінює стан сесії (RFC 2976);

REFER – запит одержувача про передавання запиту SIP (RFC 3515);

MESSAGE – передавання миттєвих повідомлень засобами SIP (RFC 3428);

UPDATE – модифікація стану сесії без зміни стану діалогу (RFC 3311).

Наприклад, у поточній версії протоколу SIP не передбачений спосіб передавання інформації управління з'єднанням або іншої інформації під час сеансу зв'язку. Для вирішення цієї задачі був запропонований новий тип запиту – INFO. Він може використовуватися у наступних випадках: для перенесення сигнальних повідомлень ТфЗК/ISDN/стільникових мереж між шлюзами протягом сеансу розмови; для перенесення сигналів DTMF протягом сеансу розмови; для перенесення білінгової інформації. Закінчивши опис запитів протоколу SIP, розглянемо в якості прикладу типовий запит типу INVITE:

INVITE sip: watson@boston.bell-tel.com SIP/2.0

Via: SIP/2.0/UDP kton.bell-tel.com

From: A. Bell

To: T. Watson

Call-ID: 3298420296@kton.bel-tel.com

Cseq: 1 INVITE

Content-Type: application/sdp

Content-Length: …

v=0

o=bell 53655765 2353687637 IN IP4 12&.3.4.5

C=IN IP4 kton.bell-tel.com

m=audio 3456 RTP/AVP 0345

У цьому прикладі користувач Bell (a.g.bell@bell-tel.com) викликає користувача Watson (watson@bell-tel.com). Запит передається до проксі-сервера (boston.bell-tel.com). У полях To і From перед адресою знаходиться запис, який викликаючий користувач бажає вивести на дисплей викликаємого користувача. У тілі повідомлення обладнання викликаючого користувача вказує у форматі протоколу SDP, що воно може приймати у порті 3456 мовну інформацію, упаковану в пакети RTP та закодовану за одним з наступних алгоритмів кодування: 0 – PCMU, 3 – GSM, 4 – G.723, 5 – DVI4.

При передаванні повідомлень протоколу SIP, упакованих у сигнальні повідомлення протоколу UDP, існує ймовірність того, що розмір запиту або відповіді виявиться більшим, ніж максимально допустимий для даної мережі, внаслідок чого відбудеться фрагментація пакету. Щоб запобігти цьому, використовується стиснутий формат імен основних заголовків, як це здійснюється у протоколі SDP. Список таких заголовків приведено у табл.4.3.

Таблиця 4.3 - Скорочені імена заголовків SIP

Стиснута форма імені	Повна форма імені
c	Content-Type
e	Content-Encoding
f	From
i	Call-ID

m	Contact (від “moved”)
l	Content-Length
s	Subject
t	To
v	Via

При написанні імен заголовків у стиснутому вигляді повідомлення INVITE матиме вигляд:

INVITE sip: watson@boston.bell-tel.com SIP/2.0

V: SIP/2.0/UDP kton.bell-tel.com

f: A. Bell

t: T. Watson

i: 3298420296@kton.bel-tel.com

Cseq: 1 INVITE

c: application/sdp

l: …

v=0

o=bell 53655765 2353687637 IN IP4 12&.3.4.5

C=IN IP4 kton.bell-tel.com

m=audio 3456 RTP/AVP 0345

Після прийому та інтерпретації запиту адресат (проксі-сервер) передає відповідь на цей запит. Зміст відповідей буває різним: підтвердження встановлення з’єднання, передавання інформації, яку запитують, повідомлення про несправності і т.д. Відповіді на запити повідомляють про результати обробки запиту або передають інформацію на запит. Структуру відповідей та їх види протокол SIP перейняв від протоколу HTTP. Визначено шість типів відповідей, які несуть різне функціональне навантаження. Тип відповіді кодується трьохзначним числом, найважливішою є перша цифра, яка визначає клас відповіді, інші дві цифри лише доповнюють першу.

Всі відповіді поділяються на дві групи: *інформаційні* та *фінальні*. Інформаційні відповіді показують, що запит знаходиться на стадії обробки. Вони кодуються

трьохзначним числом, яке починається з одиниці – **1xx**. Деякі інформаційні відповіді, наприклад, **100 Trying**, призначені для встановлення на нуль таймерів, що запускаються в обладнанні, яке передало запит. Якщо до моменту спрацювання таймера відповідь на запит не отримана, вважається, що цей запит втрачений і може (якщо захоче виробник) бути переданий повторно. Одна з розповсюджених відповідей – **180 Ringing**; за призначенням вона ідентична сигналу «Контроль посилки виклику» у ТфЗК і означає, що викликаємий користувач отримує сигнал про вхідний виклик.

Фінальні відповіді кодуються трьохзначними числами, що починаються з цифр 2, 3, 4, 5, 6. Вони означають закінчення обробки запиту і містять, за необхідністю, результат обробки запиту.

1xx – Інформаційні відповіді; показують, що запит знаходиться на стадії обробки. Найбільш розповсюджені відповіді даного типу – 100 Trying, 180 Ringing, 183 Session Progress.

2xx – Фінальні відповіді, які означають, що запит успішно оброблений. На теперішній час у даному типі визначена тільки одна відповідь – 200 OK. Значення відповіді залежить від того, на який запит вона відповідає:

- відповідь **200 OK** на запит INVITE означає, що обладнання, яке викликається, згідне приймати участь у сеансі зв’язку; у тілі відповіді вказуються функціональні можливості цього обладнання;
- відповідь **200 OK** на запит BYE означає закінчення сеансу зв’язку, у тілі відповіді не міститься ніякої інформації;
- відповідь **200 OK** на запит CANCEL означає відміну пошуку, у тілі відповіді не міститься ніякої інформації;
- відповідь **200 OK** на запит REGISTER означає, що реєстрація пройшла успішно;
- відповідь **200 OK** на запит OPTION служить для передавання відомостей про функціональні можливості обладнання, ці відомості містяться у тілі відповіді.

3xx – Фінальні відповіді, які інформують обладнання викликаючого користувача про нове місцеположення викликаємого користувача, наприклад, відповідь 302 Moved Temporary, або переносять іншу інформацію, яка може бути

використана для нового виклику:

- у відповіді **300 Multiple Choices** вказується декілька SIP-адрес, за якими можна знайти викликаємого користувача і викликаючому користувачу пропонується вибрати одну з них;
- відповідь **301 Moved Permanently** означає, що викликаємий користувач більше не знаходиться за адресою, яка вказана у запиті, і направляти запити потрібно за адресою, яка вказана у полі Contact;
- відповідь **302 Moved Temporary** означає, що користувач тимчасово (проміжок часу може бути вказаний у полі Expires) знаходиться за іншою адресою, який вказується у полі Contact.

4xx – Фінальні відповіді, які інформують про помилку під час обробки або виконання запиту, наприклад, 403 Forbidden або класична для протоколу HTTP відповідь 404 Not Found. Після отримання такої відповіді користувач не повинен передавати той самий запит без його модифікації:

- відповідь **400 Bad Request** означає, що запит не зрозумілий із-за наявності в ньому синтаксичних помилок;
- відповідь **401 Unauthorized** означає, що запит вимагає проведення процедури аутентифікації користувача. Існують різні варіанти аутентифікації, і у відповіді може бути вказано, який з них використаний у даному випадку;
- відповідь **403 Forbidden** означає, що сервер зрозумів запит, але відмовився його обслуговувати. Повторний запит не потрібно посилати. Причини можуть бути різними, наприклад, запити з цієї адреси не обслуговуються і т.д.;
- відповідь **485 Ambiguous** означає, що адреса у запиті не визначає викликаємого користувача однозначно;
- відповідь **486 Busy Here** означає, що викликаємий користувач на теперішній момент не може прийняти вхідний виклик за даною адресою. Відповідь не виключає можливості зв’язатися з користувачем за іншою адресою або залишити повідомлення у поштовій скринці для розмов.

5xx – Фінальні відповіді, які інформують про те, що запит не може бути оброблений із-за відмови сервера, 500 Server Internal Error:

- відповідь **500 Server Internal Error** означає, що сервер не має можливості обслуговувати запит із-за внутрішньої помилки. Клієнт може спробувати повторно надіслати запит через деякий час;
- відповідь **501 Not Implemented** означає, що в сервері не реалізовані функції, які необхідні для обслуговування цього запиту. Відповідь передається, наприклад, у тому випадку, коли сервер не може розпізнати тип запиту;
- відповідь **502 Bad Gateway** інформує про те, що сервер, який функціонує в якості шлюза або проксі-сервера, прийняв некоректну відповідь від сервера, до якого він направив запит;
- відповідь **503 Service Unavailable** говорить про те, що сервер не може в даний час виконати обслуговування виклику внаслідок превантаження або проведення технічного обслуговування.

6xx – Фінальні відповіді, які інформують про те, що з'єднання з викликаємим користувачем встановити неможливо:
- відповідь **600 Busy Everywhere** повідомляє, що викликаємий користувач зайнятий і не може прийняти виклик в даний момент за жодною адресою, яка є в наявності. Відповідь може вказувати час, який підходить для виклику користувача;
- відповідь **603 Decline** означає, що викликаємий користувач не може або не бажає прийняти вхідний виклик. У відповіді може бути вказаний підходящий час для виклику;
- відповідь **604 Does Not Anywhere** означає, що викликаємого користувача не існує.

У деяких випадках обладнання навіть може не знати всі коди відповідей, але воно обов'язково повинне інтерпретувати першу цифру відповіді.

Запити та відповіді на них утворюють SIP-транзакцію. Вона організовується між клієнтом та сервером і включає в себе всі повідомлення, починаючи з першого запиту, і закінчуючи фінальною відповіддю. При використанні в якості транспорту протоколу TCP всі запити та відповіді, що відносяться до однієї транзакції, передаються по одному TCP-з'єднанню.

Приклад відповіді на запит INVITE:

SIP/2.0 200 OK

Via: SIP/2.0/UDP kton.bel-tel.com

From: A. Bell

To: ;

Call-ID: 3298420296@kfcon.bell-fcel.com Cseq: 1 INVITE

Content-Type: application/sdp Content-Length: …

v=0

o=Watson 4858949 4858949 IN IP4 192.1.2.3

t=3149329600 0

c=IN IP4 bostcon.bell-tel.com

m=audio 5004 RTP/AVP 0 3

a=rtmap:0 PCMU/8000

a=rtmap:3 GSM/8000

У цьому прикладі приведено відповідь користувача Watson на запрошення взяти участь у сеансі зв'язку, яке отримане від користувача Bell. Найбільш ймовірний формат запрошення розглянутий раніше. Викликаєма сторона інформує викликаючу про те, що вона може приймати у порту 5004 мовну інформацію, яка закодована відповідно до алгоритмів кодування PCMU, GSM. Поля From, To, Via, Call-ID взяті із запиту, який показаний раніше. З прикладу видно, що це відповідь на запит INVITE з полем CSeq:1.

Протокол SIP передбачає різні алгоритми встановлення з'єднання. При цьому одні і ті ж відповіді можна інтерпретувати по-різному в залежності від конкретних ситуацій. У табл.4.4 приведені всі відповіді на запити, які визначені протоколом SIP.

Таблиця 4.4 – Відповіді на запити SIP

Код відповіді	Пояснення	Призначення
100	Trying	Запит обробляється, наприклад, сервер звертається до баз даних, але місцеполо-

		ження викликаємого користувача на теперішній момент не визначене.
180	Ringing	Місцеположення викликаємого користувача визначене. Йому надається сигнал про вхідний виклик.
181	Call Is Being Forwarded	Проксі-сервер переадресує виклик до іншого користувача.
182	Queued	Викликаємий користувач тимчасово не доступний, але вхідний виклик стоїть у черзі. Коли викликаємий користувач стане доступним, він передасть фінальну відповідь.
200	OK	Команда успішно виконана.
300	Multiple Choices	Викликаємий користувач доступний по декільком адресам. Викликаючий користувач може вибрати будь-яку з них.
301	Moved Permanently	Користувач змінив своє місцеположення, його нова адреса вказана у полі Contact.
302	Moved Temporarily	Користувач тимчасово змінив своє місцеположення, його нова адреса вказана у полі Contact.
305	Use Proxy	Викликаєма сторона може прийняти вхідний виклик тільки у тому випадку, коли він проходить через проксі-сервер. Викликаючій стороні рекомендується звернутися до проксі-сервера, адреса якого вказана у полі Contact. Відповідь передається тільки термінальним обладнанням (UAS).
380	Alternative Service	Виклик не надійшов до адресата, але існує

		альтернативний варіант обслуговування, який вказаний у тілі відповіді. Наприклад, виклик може бути переадресований до розмовної поштової скриньки.
400	Bad Bequest	У запиті виявлена синтаксична помилка.
401	Unauthorised	Необхідне виконання процедури авторизації користувача.
402	Payment Required	Необхідна попередня оплата послуг.
403	Forbidden	Запит не буде обслуговуватися сервером і не повинен передаватися повторно.
404	Not Found	Сервер не виявив викликаємого користувача в домені, який вказаний у полі Request-URI.
405	Method Not Allowed	Не дозволяється передавати запит цього виду на адресу, яка вказана у полі Request-URI. У полі Allow відповіді вказуються дозволені види запитів.
406	Not Acceptable	Відповіді, які генеруються викликаємою стороною, не будуть зрозумілі викликаючій стороні.
407	Proxy Authentication Required	Клієнт повинен підтвердити своє право доступу до проксі-серверу.
408	Request Timeout	Сервер не може передати відповідь, наприклад, вказати місцеположення викликаємого користувача, протягом проміжку часу, специфікованого у полі Expires запиту. Викликаючий користувач може повторно передати запит через деякий час.

409	Conflict	Обробка запиту REGISTER не може бути закінчена із-за конфлікту між дією, яка визначена у параметрі action запиту, та поточним станом ресурсів.
410	Gone	Сервер більше не має доступу до ресурсу, який отримав запит, і не знає, куди переадресувати запит.
411	Length Required	Необхідно вказати довжину тіла повідомлення у полі Content-Length.
413	Request Entity Too Large	Розмір запиту дуже великий для обробки.
414	Request-URI Too Large	Адреса, яка вказана у полі Request-URI, дуже велика, тому її інтерпретація неможлива.
415	Unsupported Media Type	Запит містить формат тіла повідомлення, який не підтримується.
420	Bad Extension	Сервер не зрозумів розширення протоколу, специфіковане у полі Require.
480	Temporarily not available	Викликаємий користувач тимчасово недоступний.
481	Call Beg/Transaction Does Not Exist	Надходить у відповідь на отримання запиту BYE, що не відноситься до поточних з'єднань, або запиту CANCEL, що не відноситься до поточних запитів.
482	Loop Detected	Сервер виявив, що прийнятий їм запит передається по замкнутому маршруту (у полі Via вже є адреса цього сервера).
483	Too Many Hops	Сервер виявив у полі Via, що прийнятий їм запит пройшов через велику кількість проксі-серверів, ніж дозволено у полі

		Max-Forwards.
484	Address Incomplete	Сервер прийняв запит з неповною адресою у полі To або Request-URI. Необхідна додаткова адресна інформація.
485	Ambiguous	Адреса викликаємого користувача неоднозначна. У заголовку Contact відповіді може бути список адресатів, по яким цей запит можна передати.
486	Busy Here	На теперішній момент викликаємий користувач не хоче або не може прийняти виклик за цією адресою. Відповідь не виключає можливості зв’язатися з користувачем за іншою адресою.
500	Internal Server Error	Внутрішня помилка сервера.
501	Not Implemented	У сервері не реалізовані функції, які необхідні для обслуговування запиту. Відповідь передається у тому випадку, коли сервер не може розпізнати тип отриманого ним запиту.
502	Bad Gateway	Сервер, який функціонує в якості шлюзу або проксі-сервера, приймає некоректну відповідь від сервера, до якого він направив запит.
503	Service Unavailable	Сервер не може в даний момент виконати обслуговування викликів внаслідок перенавантаження або проведення технічного обслуговування.

504	Gateway Timeout	Сервер, який функціонує в якості шлюза або проксі-сервера, протягом встановленого інтервалу часу не отримав відповіді від сервера (наприклад, від сервера визначення місцеположення), до якого він звернувся для закінчення обробки запиту.
505	SIP Version not supported	Сервер не підтримує дану версію протоколу SIP.
600	Busy Everwhere	Викликаємий користувач зайнятий і не хоче приймати виклик на даний момент. Відповідь може вказувати потрібний для виклику час.
603	Decline	Викликаємий користувач не може або не бажає приймати вхідні виклики. У відповіді може бути вказаний потрібний для виклику час.
604	Does not exist anywhere	Викликаємого користувача не існує.
606	Not Acceptable	Викликаємий користувач не може прийняти вхідний виклик із-за того, що вид інформації, який вказаний у описанні сеансу зв'язку у форматі SDP, смуга пропускання і т.д. неприйнятні.

4.4 Процеси встановлення з'єднань

Протокол SIP визначає *три основних сценарії* встановлення з'єднання: за участю проксі-сервера, за участю сервера переадресації та безпосередньо між користувачами. Сценарії відрізняються тим, як здійснюється пошук та запрошення викликаємого користувача. У першому випадку ці функції бере на

себе проксі-сервер, а викликаючому користувачу необхідно знати лише постійну SIP-адресу викликаємого користувача. У другому випадку викликаюча сторона самостійно встановлює з'єднання, а сервер переадресації лише реалізує перетворення постійної адреси викликаємого абонента у його поточну адресу. І в третьому випадку викликаючому користувачу для встановлення з'єднання необхідно знати поточну адресу викликаємого користувача.

Перераховані сценарії є найпростішими. Перед тим як виклик надійде до адресата, він може пройти через декілька проксі-серверів або спочатку прямує до сервера переадресації, а потім проходить через один або декілька проксі-серверів. Крім того, проксі-сервери можуть розмножувати запити і передавати їх за різними напрямками і т.д.

Основні алгоритми встановлення з'єднання описані у RFC 3665. Розглянемо два перші сценарії.

Встановлення з'єднання за участю сервера переадресації. Адміністратор мережі повідомляє користувачам адресу сервера переадресації. Викликаючий користувач передає запит INVITE (1) на відому йому адресу сервера переадресації і порт 5060, який використовується по умовчанню (рис.3.2). У запиті викликаючий користувач вказує адресу викликаємого користувача. Сервер переадресації виконує запит поточної адреси потрібного користувача у сервера визначення місцеположення (2), який повідомляє йому цю адресу (3). Сервер переадресації у відповіді 302 Moved temporarity передає викликаючій стороні поточну адресу викликаємого користувача (4) або може повідомити список зареєстрованих адрес викликаємого користувача і запропонувати викликаючому користувачу самому обрати одну з них. Викликаюча сторона підтверджує прийом відповіді 302 надсиланням повідомлення ACK (5).

Тепер викликаюча сторона може зв'язатися безпосередньо з викликаємою стороною. Для цього вона передає новий запит INVITE (6) з тим же ідентифікатором Call-ID, але з іншим номером CSeq. У тілі повідомлення INVITE вказуються дані про функціональні можливості викликаючої сторони у форматі протоколу SDP. Викликаєма сторона приймає запит INVITE і починає його

обробку, про що повідомляє відповіддю 100 Trying (7) зустрічному обладнанню для перезапуску його таймерів. Після закінчення обробки запиту, який надійшов, обладнання викликаємої сторони повідомляє своєму користувачу про вхідний виклик, а зустрічній станції передає відповідь 180 Ringing (8). Після прийому викликаємим користувачем вхідного виклику віддаленій стороні передається повідомлення 200 ОК (9), у якому містяться дані про функціональні можливості викликаємого терміналу у форматі протоколу SDP. Термінал викликаючого користувача підтверджує прийом відповіді запитом АСК (10). На цьому фаза встановлення з'єднання закінчена і починається фаза розмови.

По закінченню фази розмови будь-якій із сторін передається запит BYE (11), який підтверджується відповіддю 200 ОК (12).

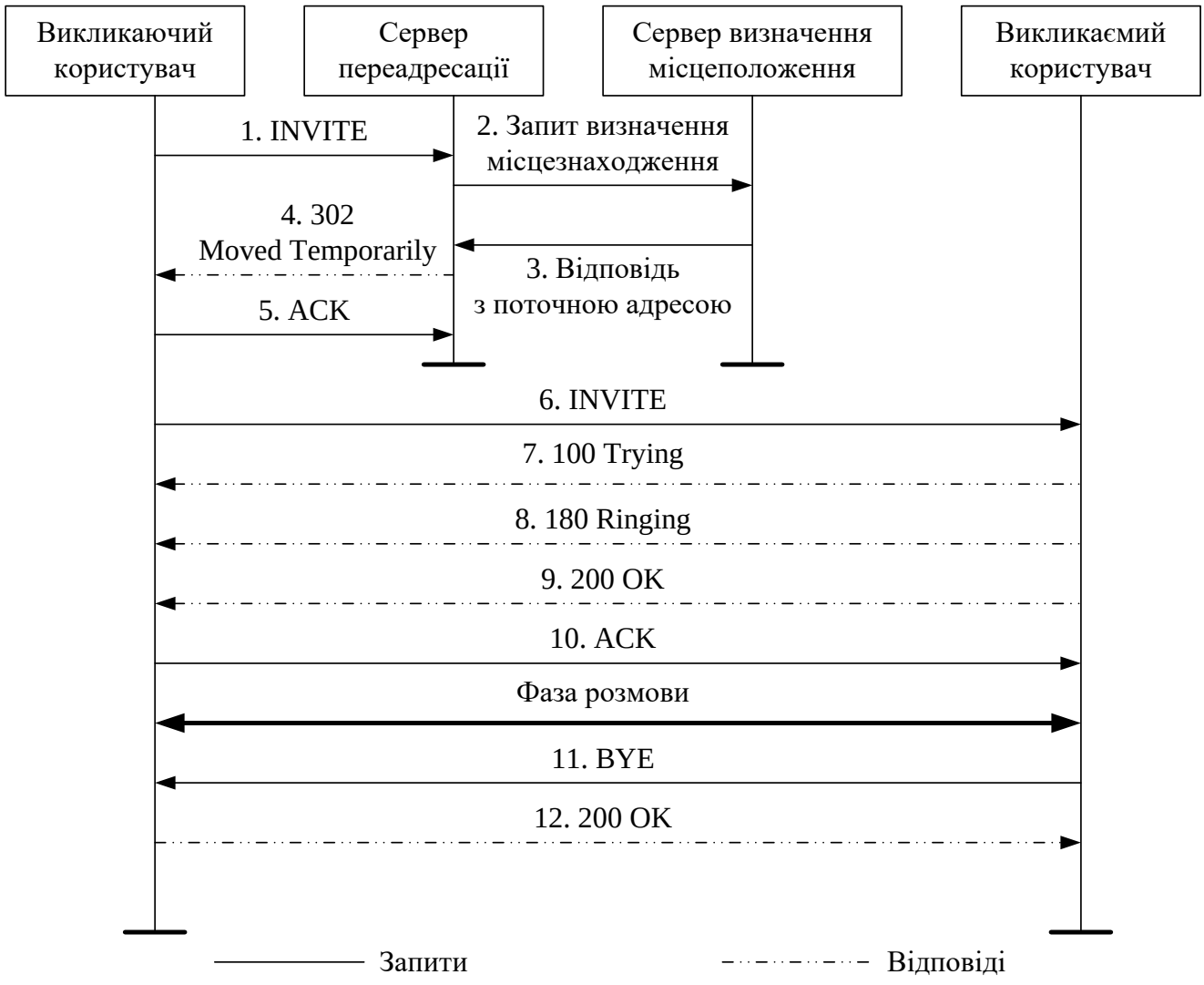


Рисунок 4.2 - Встановлення з'єднання за участю сервера переадресації

Встановлення з'єднання за участю проксі-сервера. Адміністратор мережі повідомляє адресу цього сервера користувачам. Викликаючий користувач передає запит INVITE (1) на адресу проксі-сервера і порт 5060, який використовується по умовчанню (рис.3.3). У запиті користувач вказує відому йому адресу викликаємого користувача. Проксі-сервер виконує запит поточної адреси викликаємого користувача у сервера визначення місцеположення (2), який і повідомляє йому цю адресу (3). Далі проксі-сервер передає запит INVITE безпосередньо викликаємому обладнанню (4). Знову у запиті містяться дані про функціональні можливості викликаючого терміналу, але при цьому у запит додається поле Via з адресою проксі-сервера для того, щоб відповіді на зворотньому шляху проходили через нього. Після прийому та обробки запиту викликаєме обладнання повідомляє свого користувача про вхідний виклик, а зустрічній стороні передає відповідь 180 Ringing (5), копіюючи в неї із запиту поля To, From, Call-ID, CSeq та Via. Після прийому виклику користувачем зустрічній стороні передається повідомлення 200 OK (6), що містить дані про функціональні можливості викликаємого терміналу у форматі протоколу SDP. Термінал викликаючого користувача підтверджує прийом відповіді запитом ACK (7). На цьому фаза встановлення з'єднання закінчена і починається фаза розмови.

По закінченню фази розмови одній із сторін передається запит BYE (8), який підтверджується відповіддю 200 OK (9).

Всі повідомлення проходять через проксі-сервер, який може модифікувати в них деякі поля.

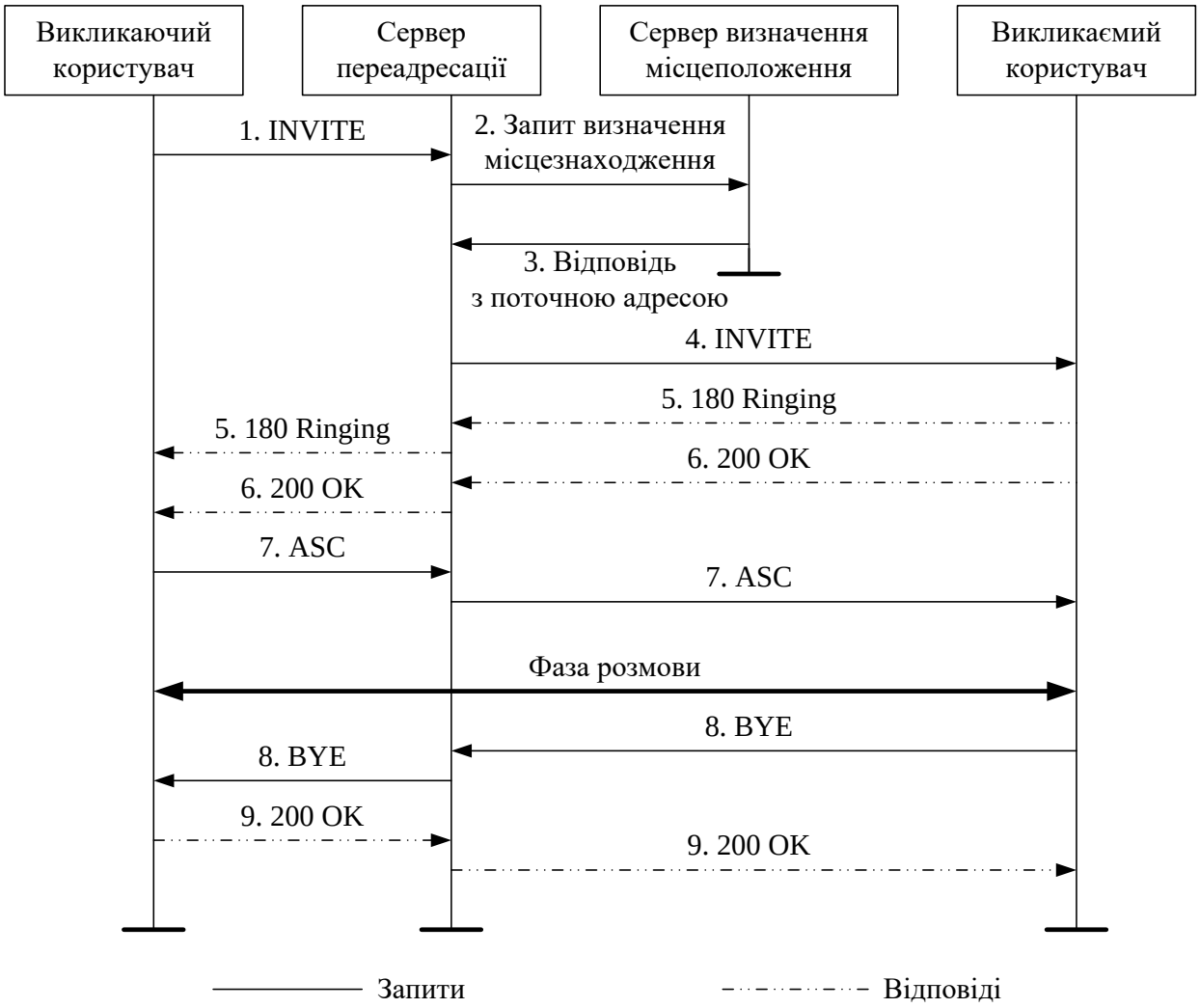


Рисунок 4.3 - Встановлення з’єднання за участю проксі-сервера

Контрольні запитання для самооцінки рівня знань

1. Які існують типи SIP-телефонів?
2. Яким чином здійснюється адресація протоколу SIP?
3. Яким чином здійснюється інтеграція SIP з IP мережами?
4. Організацію яких конференцій передбачає протокол SIP?
5. Яку структуру мають повідомлення протоколу SIP?
6. Які види заголовків використовуються у протоколі SIP?
7. Які типи запитів застосовують у теперішній версії протоколу SIP?
8. На які групи поділяються відповіді на запити?
9. Що розуміють під SIP-транзакцією?
10. Які сценарії встановлення з’єднань визначає протокол SIP?

5 АНАЛІЗ ПРАКТИЧНОГО ВИКОРИСТАННЯ ПРОТОКОЛУ SIP

5.1 Приклад побудови SIP мережі

Підводячи підсумки вищесказаного, відмітимо, що мережі SIP будуються з елементів трьох основних типів: терміналів, проксі-серверів та серверів переадресації. Структурна схема організації послуг SIP сервера представлена на рис.5.1.

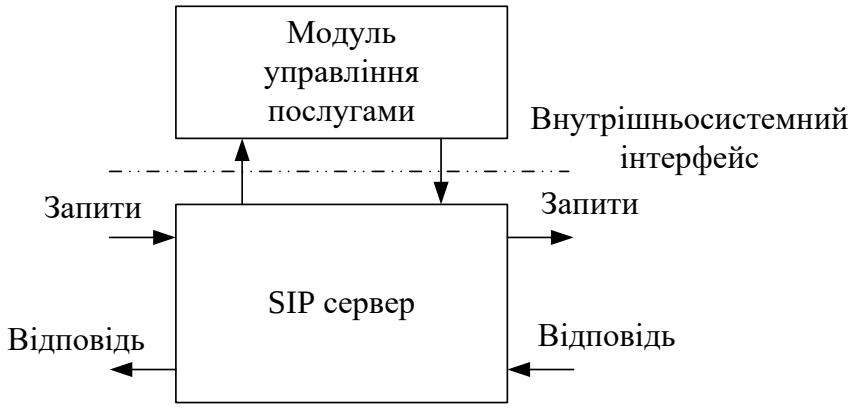


Рисунок 5.1 - Структурна схема організації послуг SIP сервера

Модуль управління послугами відповідає за надавання послуг та за загальне управління сервером. Прийняті сервером запити та відповіді надходять до модуля управління послугами, де й обробляються, на основі чого визначається реакція на отримані повідомлення. Інтерфейс людина-машина дозволяє гнучко змінювати налаштування сервера та вести моніторинг мережі.

На рис.5.2 приведений приклад можливої побудови SIP мережі. Необхідно звернути увагу на те, що SIP-сервери є окремими функціональними елементами мережі. Фізично вони можуть бути реалізовані на базі серверів локальної мережі, які, крім виконання своїх основних функцій, будуть також обробляти SIP-повідомлення. Термінали можуть бути двох типів: персональний комп’ютер із звуковою платою та програмним забезпеченням SIP-клієнта (UA) або SIP-телефон, який підключається безпосередньо до ЛОМ Ethernet (SIP-телефони, які виробляються компанією Cisco Systems). Таким чином, користувач локальної обчислювальної мережі передає всі запити до свого SIP-сервера, а сервер їх обробляє і забезпечує встановлення з’єднань. Шляхом програмування сервер

можна налаштувати на різні алгоритми роботи: він може обслуговувати частину користувачів (наприклад, керівництво підприємства або важливих осіб) за одними правилами, іншу частину – за іншими правилами. Можливо також, що сервер буде враховувати категорію і терміновість виклику, а також вести нарахування оплати за розмови.

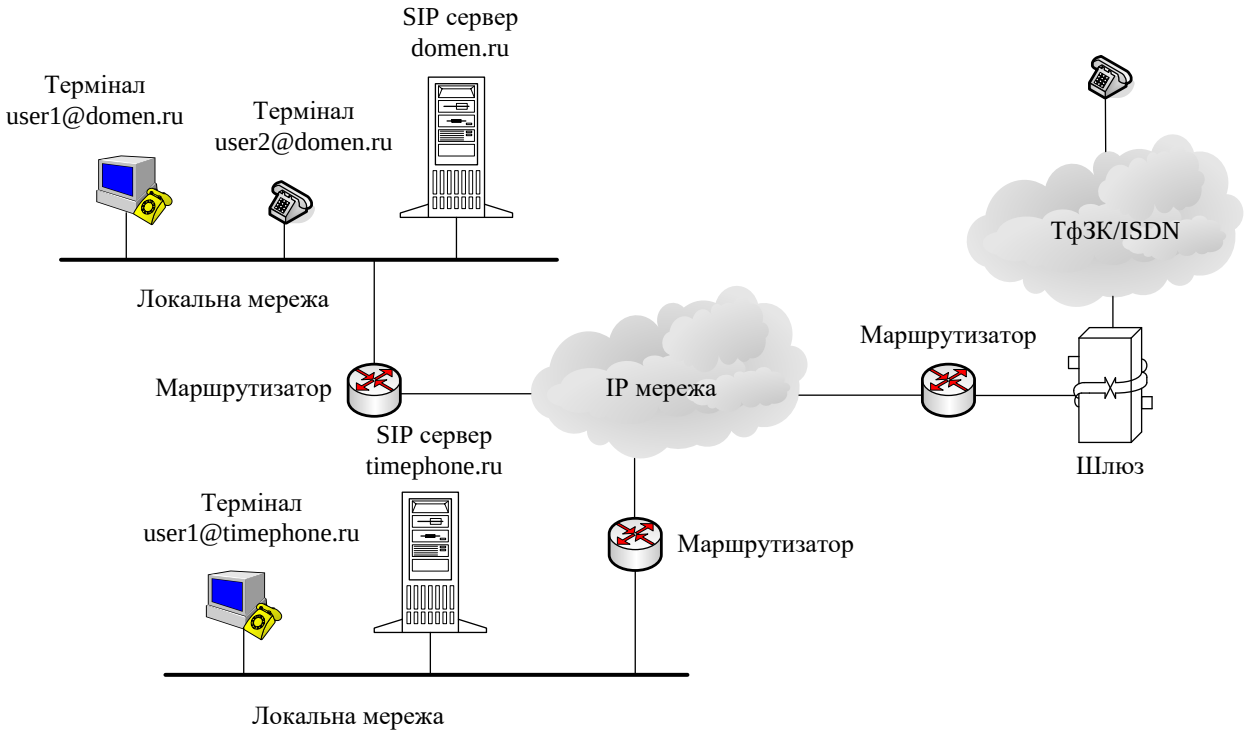


Рисунок 5.2 – Приклад побудови SIP мережі

5.2 Реалізація додаткових послуг на базі протоколу SIP

Додаткова послуга «Перемикання зв’язку» дозволяє користувачу переключити встановлене з’єднання до третьої сторони. На рис.5.3 приведений приклад реалізації цієї послуги. Користувач В встановлює зв'язок з користувачем А, який, отримавши розмову з користувачем В, переключає зв'язок до користувача С, а сам відключається.

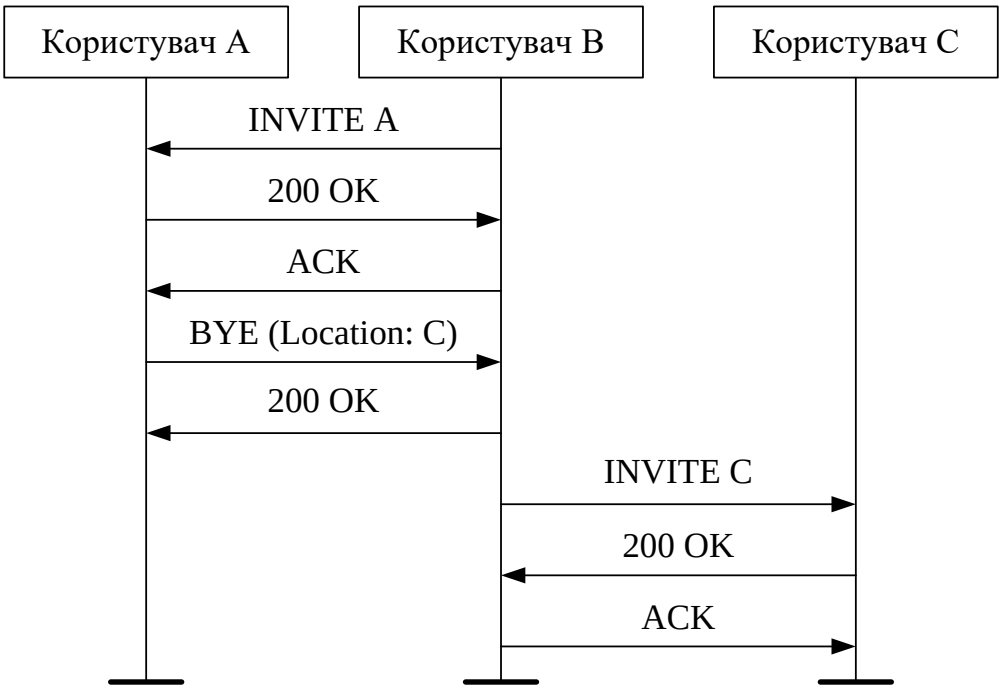


Рисунок 5.3 - Додаткова послуга «Перемикання зв’язку»

Додаткова послуга «Переадресація виклику» дозволяє користувачу призначити адресу, на яку за визначених умов необхідно направляти вхідні до нього виклики. Такими умовами можуть бути зайнятість користувача, відсутність його відповіді протягом заданого часу або і те, і інше; можлива також безумовна переадресація. Обладнання користувача, який замовив цю послугу, отримавши повідомлення INVITE B, перевіряє умови за якими воно отримане, і якщо умови вимагають переадресації, передає повідомлення INVITE із заголовком Also, вказуючи у ньому адресу користувача, до якого необхідно направити виклик. Термінал викликаючого користувача, отримавши повідомлення INVITE з таким заголовком, ініціює новий виклик за адресою, яка вказана у полі Also. У нашому випадку користувач A викликає користувача B, а термінал останнього виконує переадресацію виклику до користувача C (рис.5.4).

Рисунок 5.4 - Додаткова послуга «Переадресація виклику»

Додаткова послуга «Повідомлення про виклик під час зв’язку» дозволяє користувачу, який бере участь у телефонній розмові, отримати повідомлення про те, що до нього надійшов вхідний виклик (рис.5.5).

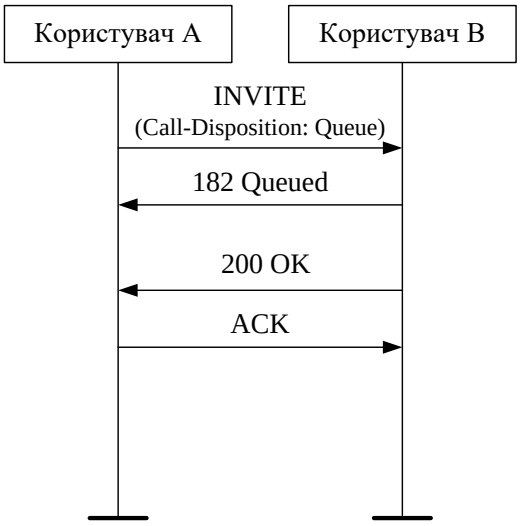


Рисунок 5.5 - Додаткова послуга «Повідомлення про виклик під час зв’язку»

Послуга реалізується за допомогою заголовка Call-Disposition, у якому міститься інструкція з обслуговування виклику. Викликаючий користувач передає запит INVITE із заголовком Call-Disposition: Queue, який інтерпретується наступним чином: викликаючому користувачу необхідно, щоб виклик був поставлений у чергу, якщо викликаємий користувач буде зайнятий. Викликаєма сторона підтверджує виконання запиту відповіддю 182 Queued, яка може

передаватися неодноразово протягом періоду очікування. Викликаємий користувач отримує повідомлення про вхідний виклик, а коли він звільняється, викликаючій стороні передається фінальна відповідь 200 OK.

5.3 Порівняльний аналіз протоколів H.323 та SIP

Протокол SIP значно молодше протоколу H.323 і досвід його використання у мережах зв'язку не порівняти з досвідом використання протоколу H.323. Існує ще один момент, на який необхідно звернути увагу. Інтенсивне впровадження технології передавання мовної інформації по IP-мережам вимагало постійного збільшення функціональних можливостей як протоколу H.323 (на теперішній час затверджена вже четверта версія протоколу), так і протоколу SIP (затверджена друга версія протоколу). Цей процес призводить до того, що переваги одного з протоколів переймаються іншим.

Обидва протоколи є результатом вирішення одних і тих же задач спеціалістами ITU-T та комітету IETF. Рішення ITU-T стало ближчим до традиційних телефонних мереж, а рішення комітету IETF базується на принципах, що складають основу мережі Інтернет.

Перейдемо безпосередньо до порівняння протоколів, яке будемо проводити за декількома критеріями.

Додаткові послуги. Набір послуг, які підтримуються обома протоколами, приблизно однаковий.

Додаткові послуги, які надаються протоколом H.323, стандартизовані в серії рекомендацій ITU-T H.450.X. Протоколом SIP правила надавання додаткових послуг не визначені, що є його серйозним недоліком, так як викликає проблеми при організації взаємодії обладнання різних фірм-виробників. Деякі спеціалісти пропонують рішення названих проблем, але ці рішення поки що не стандартизовані.

Приклади послуг, які надаються обома протоколами:

- переведення з'єднання в режим утримання (Call-hold);
- переключення зв'язку (Call Transfer);

- переадресація (Call Forwarding);
- повідомлення про новий виклик під час зв’язку (Call Waiting);
- конференція.

Розглянемо останню послугу більш детально. Протокол SIP передбачає три способи організації конференції: з використанням пристрою управління конференціями MCU, режиму багатоадресної розсилки та з’єднань учасників один з одним. В останніх двох випадках функції управління конференціями можуть бути розподілені між терміналами, тобто центральний контролер конференцій не потрібний. Це дозволяє організовувати конференції з практично необмеженою кількістю учасників.

Рекомендації H.323 передбачають ті ж три способи, але управління конференцією у всіх випадках виконується централізовано контролером конференцій MC (Multipoint Controller), який обробляє всі сигнальні повідомлення. Тому, для організації конференції, по-перше, необхідна наявність контролера MC у одного з терміналів, по-друге, учасник з активним контролером MC не може вийти із конференції. Крім того, при великій кількості учасників конференції MC може стати «вузьким місцем». Правда, у третій версії рекомендації ITU-T H.323 прийняте положення про каскадне з’єднання контролерів, але виробники цю версію у своєму обладнанні поки що не реалізували. Перевагою протоколу H.323 у частині організації конференцій є більш потужні засоби контролю конференцій.

Протокол SIP спочатку був орієнтований на використання у IP-мережах з підтримкою режиму багатоадресної розсилки інформації (прикладом може бути мережа Mbone, яка має тисячі постійних користувачів). Цей механізм використовується у протоколі SIP не тільки для доставки мовної інформації (як у протоколі H.323), але і для перенесення сигнальних повідомлень. Наприклад, у режимі багатоадресної розсилки може передаватися повідомлення INVITE, що полегшує визначення місцеположення користувача і є дуже зручним для центрів обслуговування викликів (Call-center) при організації групових повідомлень.

У той же час, протокол H.323 надає більше можливостей управління

послугами, як у частині аутентифікації та обліку, так і у частині контролю використання ресурсів мережі. Можливості протоколу SIP у цій частині менші, і вибір оператором цього протоколу може бути ознакою того, що для оператора важливіша технічна інтеграція послуг, ніж можливості управління послугами.

Протокол SIP передбачає можливість організації зв'язку третьої сторони (third-party call control). Ця функція дозволяє реалізувати такі послуги, як набір номеру секретарем для менеджера та супроводження виклику оператором центру обслуговування викликів. Подібні послуги передбачені і протоколом H.323, але реалізація їх дещо складніша.

У протоколі SIP є можливість вказувати пріоритети в обслуговуванні викликів, оскільки у багатьох країнах існують вимоги надавати переваги деяким користувачам. У протоколі H.323 такої можливості немає. Крім того, користувач SIP-мережі може реєструвати декілька своїх адрес і вказувати пріоритетність кожної з них.

Персональна мобільність користувачів. Протокол SIP має хороший набір засобів підтримки персональної мобільності користувачів, до яких входить переадресація виклику до нового місцеположення користувача, одночасний пошук за декількома напрямками (з виявленням зациклення маршрутів) і т.д. У протоколі SIP це здійснюється шляхом реєстрації на сервері визначення місцеположення, взаємодія з яким може підтримуватися будь-яким протоколом. Персональна мобільність підтримується і протоколом H.323, але менш гнучко.

Розширюваність протоколу. Необхідною і важливою в умовах еволюціонуючого ринку є можливість введення нових версій протоколів і забезпечення сумісності різних версій одного протоколу. Розширюваність (extensibility) протоколу забезпечується: узгодженням параметрів; стандартизацією кодеків; модульністю архітектури.

Протокол SIP досить просто забезпечує сумісність різних версій. Поля, які не зрозумілі обладнанню, просто ігноруються. Це зменшує складність протоколу, а також полегшує обробку повідомлень та впровадження нових послуг. Клієнт може запросити будь-яку послугу за допомогою заголовка Require. Сервер, який

отримав запит з таким заголовком перевіряє, чи підтримує він цю послугу і якщо не підтримує, повідомляє про це у своїй відповіді, що містить список послуг, які підтримуються.

У випадку необхідності, в організації IANA (Internet Assigned Numbers Authority) можуть бути зареєстровані нові заголовки. Для реєстрації в IANA відправляється запит з іменем заголовку та його призначенням. Вказаним чином розробник може впроваджувати нові послуги.

Для забезпечення сумісності версій протоколу SIP визначено шість основних типів запитів і шість класів відповідей на запити. Так як визначаючою у кодах відповідей є перша цифра, обладнання може вказувати та інтерпретувати лише її, а інші цифри коду тільки доповнюють зміст, їх аналіз не є обов'язковим.

Пізніші версії протоколу H.323 повинні підтримувати більш ранні версії. Але можлива ситуація, коли виробники підтримують тільки одну версію, щоб зменшити розмір повідомлень та полегшити їх декодування.

Нові функціональні можливості вводяться у протокол H.323 за допомогою поля NonStandardParameter. Поле містить код виробника, за ним – код послуги, який дійсний тільки для цього виробника. Це дозволяє виробнику розширювати послуги, але має деякі обмеження. По-перше, неможна отримати запит інформації у викликаємої сторони про послуги, які нею підтримуються, по-друге, неможна добавити нове значення вже існуючого параметру. Існують також проблеми, які пов'язані із забезпеченням взаємодії обладнання різних виробників.

На розширення можливостей протоколу як і на сумісність обладнання, що його реалізує, впливає і набір кодеків, який підтримується протоколом. У протоколі SIP для передавання інформації про функціональні можливості терміналу використовується протокол SDP. Якщо виробник підтримує якийсь особливий алгоритм кодування, цей алгоритм просто реєструється в організації IANA.

У протоколі H.323 всі кодеки повинні бути стандартизовані. Тому прикладення з нестандартними алгоритмами кодування можуть мати проблеми при реалізації їх на базі протоколу H.323.

Протокол SIP складається з набору закінчених компонентів (модулів), які

можуть замінюватися в залежності від вимог і можуть працювати незалежно один від одного. Цей набір включає в себе модулі підтримки сигналізації для базового з'єднання, для реєстрації та для визначення місцеположення користувача, які не залежать від модулів підтримки якості обслуговування (QoS), роботи з директоріями, описання сеансів зв'язку, розгортання послуг (service discovery) та управління конфігурацією.

Архітектура протоколу H.323 монолітна і представляє собою інтегрований набір протоколів для одного застосування. Протокол складається із трьох основних складових і для створення нової послуги може знадобитися модифікація кожної складової.

Масштабованість мережі (scalability). Сервер SIP за замовчуванням не зберігає відомостей про поточні сеанси зв'язку і тому може обробити більше викликів, ніж протокол H.323, який зберігає ці відомості (statefull). Разом з тим відсутність таких відомостей, на думку деяких спеціалістів, може викликати складнощі при організації взаємодії мережі IP-телефонії з ТфЗК [10].

Необхідно також враховувати зонову архітектуру мережі H.323, яка дозволяє забезпечити розширюваність мережі шляхом збільшення кількості зон.

Час встановлення з'єднання. Наступною суттєвою характеристикою протоколів є час, який необхідний, щоб встановити з'єднання. У запиті INVITE протоколу SIP міститься вся необхідна для встановлення з'єднання інформація, включаючи опис функціональних можливостей терміналу. Таким чином, у протоколі SIP для встановлення з'єднання необхідна одна транзакція, а у протоколі H.323 необхідно здійснювати обмін повідомленнями декілька разів. За цими причинами витрати часу на встановлення з'єднання у протоколі SIP значно менші, ніж у протоколі H.323. Правда, при використанні інкапсуляції повідомлень H.245 у повідомлення H.225 або процедури Fast Connect час встановлення з'єднання значно зменшується.

Крім того, на час встановлення з'єднання впливає також і транспортний протокол, який знаходиться нижче та переносить сигнальну інформацію. Ранішні версії протоколу H.323 передбачали використання для перенесення сигнальних

повідомлень H.225 та H.245 тільки протокол TCP, і лише третя версія протоколу передбачає можливість використання протоколу UDP. Протоколом SIP використання протоколів TCP та UDP передбачалося з самого початку.

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

Адресація. До системних характеристик відноситься і передбачена протоколами адресація. Використання URL є сильною стороною протоколу SIP і дозволяє легко інтегрувати його в існуючу систему DNS-серверів та впроваджувати обладнання, що працює в IP-мережах. Користувач отримує можливість перенаправляти виклики на Web-сторінки або використовувати електронну пошту. Адресою у SIP може також бути телефонний номер з адресою шлюзу, який використовується.

У протоколі H.323 використовуються транспортні адреси та alias-адреси. В якості останніх можуть використовуватися телефонний номер, ім'я користувача або адреса електронної пошти.

Складність протоколу. Протокол H.323 складніший, ніж протокол SIP. Загальний об'єм специфікацій протоколу H.323 складає приблизно 700 сторінок. Об'єм специфікацій протоколу SIP складає 150 сторінок. Протокол H.323 використовує велику кількість інформаційних полів у повідомленнях (до 100), при декількох десятках таких же полів у протоколі SIP. При цьому для організації базового з'єднання у протоколі SIP достатньо використати три запита (INVITE, BYE, ACK) та декілька полів (To, From, Call-ID, CSeq). Протокол SIP структурований відносно запитів і відповідей, його прихильники повідомляють про нього як про більш простий порівняно з H.323. Але деякі схильні вважати, що в той час як спочатку метою SIP була простота, у своєму сьогоднішньому вигляді він став таким же складним як і H.323. Інші вважають, що SIP – протокол без станів, який тим самим дає можливість легко реалізувати відновлення при відмові та інші можливості, які ускладнені в протоколах із станами, таких як H.323. Виходячи з цього, протокол SIP має пріоритет. SIP та H.323 не обмежені

голосовим зв’язком, вони можуть обслуговувати будь-який сеанс зв’язку від голосового до відеосеансу або прикладень майбутнього (табл.5.1).

Таблиця 5.1 – Параметри порівняння протоколів SIP та H.323

Параметр порівняння	SIP	H.323
Додаткові послуги	Набір послуг, які підтримуються обома протоколами, приблизно однаковий	
Персональна мобільність користувачів	Хороший набір засобів підтримки мобільності	Персональна мобільність підтримується, але менш гнучко
Розширюваність протоколу	Зручна розширюваність, проста сумісність з попередніми версіями	Розширюваність підтримується, але є ряд труднощів
Масштабність мережі	Обидва протоколи забезпечують хорошу масштабність мережі	
Час встановлення з’єднання	Достатньо однієї транзакції	Необхідно декілька транзакцій
Складність протоколу	Простий, мало запитів, текстовий формат повідомлень	Складний, багато запитів і протоколів, двійкове представлення повідомлень

Протокол SIP використовує текстовий формат повідомлень як і протокол HTTP. Це полегшує синтаксичний аналіз та генерацію коду, дозволяє реалізувати протокол на базі будь-якої мови програмування, полегшує експлуатаційне управління, дає можливість ручного введення деяких полів, полегшує аналіз повідомлень. Назва заголовків SIP-повідомлень вказує їх значення.

Протокол H.323 використовує двійкове представлення своїх повідомлень на базі мови ASN.1, тому їх безпосереднє читання ускладнене. Для кодування і декодування повідомлень необхідно використовувати компілятор ASN.1. Але, в той же час, обробка повідомлень, представлених у двійковому вигляді,

відбувається швидше.

Досить складною є взаємодія протоколу H.323 з міжмережним екраном (firewall). Крім того, у протоколі H.323 передбачене дублювання функцій. Так, наприклад, обидва протоколи H.245 і RTCP мають засоби управління конференцією та здійснення зворотнього зв'язку.

На основі приведеного вище порівняння можна зробити висновок про те, що протокол SIP більше підходить для використання Інтернет-постачальниками, оскільки вони розглядають послуги IP-телефонії лише як частину набору своїх послуг.

Оператори телефонного зв'язку для яких послуги Інтернет не є першочерговими, скоріш за все, будуть орієнтуватися на протокол H.323, оскільки мережа, яка побудована на базі рекомендацій H.323, представляється їм добре знайомою мережею ISDN, яка накладена на IP-мережу.

Необхідно враховувати, що на теперішній час багато фірм-виробників та постачальників послуг вже вклали значні кошти у обладнання H.323, яке успішно функціонує на мережах.

Таким чином, відповідь на питання, який з протоколів має перевагу у використанні, буде залежати від мети бізнесу та необхідних функціональних можливостей. Скоріш за все, ці варіанти не треба розглядати як конкуруючі, а як призначені для різних областей ринку послуг, оскільки вони можуть працювати паралельно та взаємодіяти через спеціальний шлюз. Проілюструємо це твердження наступним прикладом. На теперішній час ринок послуг все більше націлюється на послуги з доплатою за додаткові можливості (value added), і простота їх надавання дає реальні переваги. Так, використання SIP у будь-якому приватному домені надає можливість більш гнучкого надавання послуг, а наявність засобів, які забезпечують перехід від протоколу SIP до протоколу H.323, гарантує взаємодію з областями, які використовують інші рішення. У табл.5.2 приведений варіант можливого обміну повідомленнями.

Таблиця 5.2 – Алгоритм встановлення з’єднання за участю шлюзу H.323/SIP

Крок	H.323 – сторона шлюзу	SIP – сторона шлюзу	Коментарії
1	→ Setup (з процедурою Faststart)		Містить опис можливостей прийому інформації.
2	← Call procceding		Підтвердження проксі-сервером прийому повідомлення SETAP.
3		INVITE →	Містить опис можливостей прийому інформації у форматі SDP.
4		← 180 Ringing	Повідомлення викликаючого користувача про те, що викликаємому користувачу передається сигнал про вхідний виклик.
5	← Alerting		
6		200 OK ←	Викликаємий користувач прийняв вхідний виклик, повідомлення містить опис можливостей прийому інформації.
7	← Connect		
8		ACK →	
	Телефонна розмова		
N		BYE ←	Розмова закінчена.
N+1	← Release complete		
N+2		200 OK →	

Якщо протягом фази розмови обладнанню H.323 необхідно відкрити нові логічні канали, шлюз передає нове повідомлення INVITE терміналу SIP, як показано у табл.5.3.

Таблиця 5.3 – Відкриття нових логічних каналів

Крок	H.323 – сторона шлюзу	SIP – сторона шлюзу	Коментарії
	→ Open Logical Channel		
		INVITE →	Той же ідентифікатор з'єднання, що і в попередньому повідомленні INVITE (але номер Cseq – збільшений).
		200 OK ←	Опис нового каналу у форматі SDP. Містить опис нового каналу у форматі SDP.
	← Open Logical Channel ACK		

5.4 Практичне використання протоколу

Багато ISP (Sipnet, Telphin, Externet та ін.) підтримують протокол SIP для надавання послуг телефонного зв'язку. За невелику оплату абонент може завести один або декілька телефонних номерів. Виклики всередині мережі та «партнерських» мережах безкоштовні, а виклики до інших мереж значно дешевше, ніж звичайні телефонні виклики. Крім того, номер SIP не прив'язаний до визначеного географічного місцеположення і може використовуватися у будь-якому місці, де є широкосмуговий доступ до мережі Інтернет.

Практично, у всіх сучасних комунікаційних системах виробництва DeTeWe реалізована вбудована підтримка SIP-телефонії з використанням системних або стандартних телефонних терміналів: аналогових, цифрових, IP-телефонів, DECT

трубок та ін. У якості прикладів таких систем можна привести обладнання сімейства OpenCom 1000, OpenCom 100, OpenCom X320, OpenMobility SIP та ін. Для доступу до SIP зв'язку може використовуватися, наприклад, виділений код доступу або послуга автоматичної маршрутизації LCR.

Виклик абонента іншого підрозділу підприємства з використанням IP-телефонії на базі SIP дуже простий і не потребує дорогого обладнання. Єдина складність на сьогоднішній день – відсутність повсюдного доступу до xDSL ліній. Також відсутня можливість донабору номера визначеного абонента і необхідно організовувати окремий SIP номер для кожного абонента корпоративної мережі. Але вартість SIP номера невелика, і це не є великою перешкодою для впровадження SIP.

Використання SIP у будь-якому приватному домені надає можливість більш гнучкого надавання послуг, а наявність засобів, які забезпечують перехід від протоколу SIP до протоколу H.323, гарантує взаємодію з областями, які використовують інші рішення. Крім того, номер SIP не прив'язаний до визначеного географічного місцеположення і може використовуватися у будь-якому місці, де є широкосмуговий доступ до мережі Інтернет.

Практично, у всіх сучасних комунікаційних системах виробництва DeTeWe реалізована вбудована підтримка SIP-телефонії з використанням системних або стандартних телефонних терміналів: аналогових, цифрових, IP-телефонів, DECT трубок та ін. Виклик абонента іншого підрозділу підприємства з використанням IP-телефонії на базі SIP дуже простий і не потребує дорогого обладнання. Індивідуальний SIP номер для кожного співробітника компанії дозволить, у випадку необхідності, дуже гнучко змінити конфігурацію робочого місця, організувати віддалену роботу, що дуже важливо для співробітників, які часто знаходяться у відрядженнях.

Контрольні запитання для самооцінки рівня знань

1. Яким чином здійснюється реалізація додаткових послуг на базі протоколу SIP?
2. Які способи організації конференції передбачає протокол SIP?
3. Які засоби підтримки персональної мобільності користувачів використовує протокол SIP?
4. Яким чином здійснюється оцінка часу встановлення з’єднання по протоколу SIP?
5. Яким чином здійснюється організація послуг SIP сервера?
6. Яким чином здійснюється встановлення з’єднання за участю сервера переадресації?
7. Яким чином встановлюється з’єднання за участю проксі-сервера?
8. За якими параметрами виконують порівняння протоколів SIP та H.323?
9. Яке практичне використання має протокол SIP?
10. Які послуги надаються протоколами H.323 та SIP?

СПИСОК СКОРОЧЕНЬ

AP (Access Point) – точка доступу;

DL (Downlink) – прямий напрямок зв’язку;

IP (Internet Protocol) – Інтернет-протокол;

ISO (International Organization for Standartization) – Міжнародна організація по стандартизації;

GPRS (General Packet Radio Service) – служба пакетного передавання даних;

LAN (Local Area Network) – локальна мережа;

LLC (Logical Link Control) – управління логічним каналом;

MAC (Media Access Control) – управління доступом до середовища;

OSI (Open Systems Interconnection) – Модель взаємодії відкритих систем;

PAN (Personal Area Network) – персональна мережа;

PHY (Physical) – фізичний рівень;

Proxy Servers – проксі-сервер;

PSTN (Public Switched Telephone Network) – телефонна мережа загального користування;

RSVP (Resource Reservation Protocol) – протокол резервування ресурсів;

RTP (Real Time Transport Protocol) – транспортний протокол реального часу;

SDP (Session Description Protocol) – протокол описання параметрів зв’язку;

SDU (Service Data Unit) – сервісний блок даних;

SIP (Session Initiation Protocol) – протокол встановлення сеансу зв’язку;

TDM (Time Division Multiplexing) – часове мультиплексування;

UA (User Agent) – агент користувача;

UAC (User Agent Client) – клієнт агента користувача;

UL (Uplink) – зворотній напрямок зв’язку;

UAS (User Agent Server) – сервер агента користувача;

UMTS (Universal Mobile Telecommunication System) – універсальна мобільна телекомунікаційна система;

UTP (Unshielded Twisted Pair) – неекранована вита пара.

ЛІТЕРАТУРА

1. Дымарский Я.С., Крутякова Н.П., Яновский Г.Г. Управление сетями связи: принципы, протоколы, прикладные задачи. – М.: НТЦ «Мобильные коммуникации », 2003. – 384с.

2. Стеклов В.К., Беркман Л.Н. Телекомунікаційні мережі. – К.: Техніка, 2001. – 650с.

3. Джон К. Беллами. Цифровая телефония: Пер. с англ. – М.: Эко-Трендз, 2004. – 640с.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 3-е изд. – СПб.: Питер, 2006. – 958с.

5. Farago A., Myers A.D., Syrotiuk V.R., Zaruba G.V. Meta-MAC protocols: automatic combination of MAC protocols to optimize performance for unknown conditions // IEEE JSAC, vol. 18, №9, sept. 2000.

6. Росляков А.В., Самсонов М.Ю., Шибаева И.В. IP-телефония. М.: Эко-Трендз, 2003.

7. International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), 1997. ITU-T. G.811: Timing characteristics of primary reference clock.

8. Стеклов В.К., Кільчицький Є.В. Основи управління мережами та послугами телекомунікацій. – К.: Техніка. – 2004. – С.438.

9. Ш. Вегешна. Качество обслуживания в сетях IP – М.: Вильямс, 2003. – 368с.

10. 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.

11. Цифровые системы коммутации для ГТС/под ред. В.Г. Карташевского и А.В. Рослякова. – М.: Эко-Трендз, 2008. – 352с.

12. 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.

13. Гостєв В.І., Кунах Н.І., Ткаленко О.М., Невдачина О.В. Мережні технології**.** Навч. посібник підготовлено для студентів вищих навчальних закладів – Київ: ДУІКТ, 2012. – 101с.

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

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

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

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

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

19. 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.

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

21. Гольдштейн, Б.С. Протокол SIP / Б.С. Гольдштейн, А.А. Зарубин, В.В.Саморезов; Серия «Телекоммуникационные протоколы». – СПб. : БХВ – СПб, 2009.

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

23. CCNA™ Cisco ® Certified Network Associate Study Guide Second Edition Todd Lammle Copyright 2000.

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