Plag

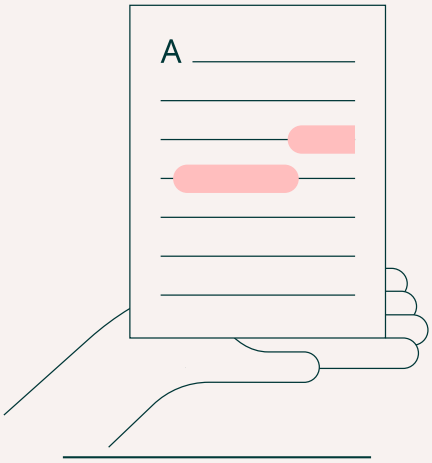
Звіт про оригінальність

● Оцінка схожості 6%

● Ризик плагіату ВИСОКИЙ

Olga Kagalo 2025-06-19 22:59

Посилання на звіт: 10mCH / Посилання користувача: qEAc



Ось вона –
Ваша звіт про оригінальність!

Ми раді повідомити, що перевірка вашого документа завершена, і результати вже готові! Наші алгоритми старанно працювали, щоб знайти збіги в наших базах даних.

На наступних сторінках ви знайдете результати перевірки:

Бали
Збіги
Посилання

Ваш документ було перевірено за такими джерелами:

- ✓ База даних інтернет-джерел
- ✓ База даних наукових статей
- ○ Глибока перевірка (наш вдосконалений алгоритм)

Бали

Збіги тексту	6%
Перефразування	0%
Цитований текст	0%
Неправильне цитування	0%
Збігів не знайдено	94%

Ризик плагіату ВИСОКИЙ

Ризик плагіату вказує, як збіги тексту розподілені по документу. Вищий ризик виникає, коли збіги з'являються близько один до одного, наприклад, у тому самому абзаці або розділі.

Оцінка схожості 6%

Оцінка схожості показує, скільки слів або символів у вашому документі збігаються з текстами інших документів, включаючи перефразовані тексти або неправильні цитати.

Збіги

ВСТУП

Сьогодні існує безліч джерел — як в Інтернеті, так і в друкованих виданнях — де можна знайти інформацію про мережу Інтернет та протокол IP (Internet Protocol). У цьому тексті подано лише основні принципи, які допоможуть зрозуміти, як IP-протокол і сам Інтернет використовуються для передавання голосових повідомлень.

Інтернет є частиною великої інформаційної інфраструктури, яку можна охарактеризувати такими ознаками:

він має єдиний логічний простір адрес, що базується на IP-протоколі або його новіших версіях;здатний забезпечити зв’язок завдяки TCP/IP або сумісним з ним протоколам;дозволяє отримувати чи надавати сервіси високого рівня, які ґрунтуються на цьому зв’язку та супутній інфраструктурі.

Коли створювали Інтернет, розробники спиралися на два головні принципи:

побудувати одну фізичну мережу, яка б задовольнила всі потреби користувачів, практично неможливо;тому потрібна універсальна система, яка дозволила б різним користувачам встановлювати зв'язки між собою незалежно від технічних особливостей їхніх мереж.

У різних фізичних мережах можуть використовуватись різні технології: Ethernet, Token Ring, FDDI, ISDN, точка-точка, ATM, або навіть бездротові рішення. Щоб усі ці різні технології могли працювати разом, між прикладними програмами і конкретними мережевими інтерфейсами створюється програмне забезпечення, яке забезпечує взаємодію. Користувачі ж цього процесу не помічають — для них це виглядає як робота в єдиній великій мережі. Такий підхід і став основою того, що ми сьогодні називаємо технологією Інтернет.

Ключовим елементом у побудові Інтернету є протокол IP, а для з'єднання між різними мережами використовуються маршрутизатори. Це спеціалізовані комп’ютери, які об’єднують окремі мережі та пересилають пакети даних з однієї в іншу завдяки відповідному ПЗ.

Однією з ключових особливостей Інтернету є його децентралізована архітектура. Він не має єдиного центру управління або контролю.

Нову мережу можна легко приєднати без необхідності прямого зв’язку з кожною вже наявною. Маршрутизатори працюють так, що мають уявлення про мережеву структуру поза межами своїх безпосередніх з’єднань і можуть направляти пакети за потрібною адресою, використовуючи універсальну систему ідентифікації. Це дозволяє будь-яким двом пристроям у мережі встановлювати зв’язок один з одним незалежно від їхнього розташування чи внутрішньої структури мереж.

В основі роботи Інтернету лежить ідея незалежності користувача від конкретної фізичної мережі. Це означає, що має існувати багато різних способів з'єднання та передавання даних, які працюватимуть однаково ефективно незалежно від використовуваної технології.

Для звичайного користувача Інтернет виглядає як одна велика віртуальна мережа, хоча насправді вона складається з безлічі взаємопов’язаних фізичних мереж. Завдяки цьому з’єднання між комп’ютерами здається прозорим — немає потреби знати, як саме фізично з’єднані машини. Щоб це працювало, кожен комп’ютер повинен мати відповідне програмне забезпечення для доступу до Інтернету, яке дозволяє прикладним програмам взаємодіяти з мережею як з єдиним цілим.

1 ЗАГАЛЬНІ ПРИНЦИПИ IP-ТЕЛЕФОНІЇ

1.1 Мережа Інтернет і протокол IP

Інтернет побудований за принципом рівноправності всіх мереж, що входять до його складу: будь-яка мережа — незалежно від її фізичних характеристик, відстаней чи розміру пакетів — вважається повноцінною частиною Інтернету. На схемах (наприклад, рисунок 1.2) усі типи мереж (локальні, глобальні, точка-точка) позначаються однаково, що підкреслює цю рівність.

Рівень мережевого інтерфейсу відповідає за організацію з’єднання в конкретній фізичній мережі. Тут взаємодіють драйвери пристроїв, мережеві плати та інше обладнання. Наступний рівень — мережевий — є основою TCP/IP-архітектури. На ньому реалізуються ключові функції, зокрема маршрутизація даних між різними мережами. Головним протоколом цього рівня є IP, який відповідає за доставку пакетів з одного пристрою до іншого, незалежно від того, скільки мереж та маршрутизаторів між ними.

Протокол IP задає формат пакета — так званої дейтаграми — і визначає, як дані мають передаватися по мережі. Він не гарантує, що пакет дійде до адресата у правильному порядку або взагалі не загубиться, оскільки IP не має вбудованих механізмів перевірки чи повторної передачі. Замість цього він просто «доставляє» — а вже в разі помилок на

допомогу приходить інший протокол, ICMP, який повідомляє про збої.

Надійна передача даних забезпечується на транспортному рівні. Тут працюють TCP і UDP — протоколи, які встановлюють зв’язок між відправником і отримувачем. TCP гарантує доставку без втрат і в правильному порядку, тоді як UDP — легший, але не такий надійний.

Прикладний рівень — це те, з чим взаємодіє користувач безпосередньо. Програми типу браузера, поштового клієнта або клієнта FTP використовують протоколи цього рівня, не переймаючись тим, як дані передаються нижчими рівнями. Наприклад, Telnet, FTP, HTTP чи SMTP — це лише частина списку відомих прикладних протоколів.

Ще одна сильна сторона Інтернету — його прозорість для прикладних програм. Вони працюють однаково, навіть якщо клієнт сидить у мережі Ethernet, а сервер — у Token Ring. Між ними може бути безліч маршрутизаторів та різних проміжних мереж, але додаток цього не бачить — для нього це одна суцільна мережа. Саме завдяки цьому Інтернет настільки універсальний.

На основі протоколу IP сьогодні будуються не лише глобальні, а й локальні або корпоративні мережі, які можуть працювати як незалежно, так і з доступом до Інтернету. Цей підхід відкриває широкі можливості не лише для передавання текстових або цифрових даних, а й для трансляції мультимедійного контенту — наприклад, відео чи голосу. Останніми роками IP-мережі активно використовуються для передавання голосових повідомлень, що значно розширює сферу їх застосування.

1.2 Основні особливості IPтелефонії

У професійній літературі зазвичай використовують три терміни для опису передачі голосу через IPмережі:IPтелефонія;Voice over IP (VoIP); Інтернеттелефонія.

IPтелефонія — це будьяка технологія, що дозволяє передавати голос чи факс у режимі реального часу через мережу з IPкомутацією (наприклад, Інтернет). За кордоном цей процес найчастіше називають VoIP — і з точки зору технічних рішень IPтелефонія й VoIP фактично одне й те саме.

Інтернеттелефонія — це різновид IPтелефонії, коли канали зв’язку, що використовуються для передачі голосових даних — або на шляху від абонента до оператора, або на магістральному рівні — працюють саме через загальнодоступний Інтернет.

Міжнародна термінологія досі остаточно не визначена. Наприклад, на семінарі Міжнародного союзу електрозв'язку (ITU, Женева, 14–16 червня 2000) запропонували

поділ:

Інтернеттелефонія — це передача голосу у публічних, часто неадміністрованих мережах;

VoIP — це подібні сервіси, але в надійно керованих корпоративних мережах.

У деяких країнах розрізняють види IPтелефонії за показниками якості і затримки:

IPтелефонія як окремий сервіс, дешевша за традиційну телефонію.

IPтелефонія як базова, проста послуга в межах ширшого пакету комунікацій (повідомлення, відео, дані).

1.3 Як працює пакетна передача голосу

У традиційних телефонних мережах для кожної розмови відкривається окремий канал — постійне з’єднання через АТС.

Аналоговий сигнал з пропускною здатністю 3,1 кГц надходить до АТС, де його мультиплексують з іншими користувацькими сигналами для подальшого транспортування до іншої АТС. Там він демультиплексується і доставляється кінцевому адресату. Однак, цей підхід неефективно використовує канал: навіть під час пауз у розмові смуга пропускання залишається зайнятою, попри відсутність передачі даних.

Цифрова революція докорінно змінила цей підхід: у мережах з пакетною комутацією інформація передається не як безперервний потік, а ділиться на незалежні пакети, фрейми або клітини. Ці пакети рухаються через мережу через віртуальні канали — без прив'язки до конкретного фізичного з'єднання — і складаються на стороні приймача згідно з інформацією з їх заголовків.

У IPмережах усі типи даних — голос, текст, відео, програми — передаються в пакетах. Кожен комп’ютер має IPадресу, і на основі цієї адреси пакети маршрутизуються до потрібного одержувача. Якщо в мережі трапляються несправності чи перевантаження, IPмережі можуть обирати інший маршрут — і це відбувається прозоро для користувачів.

Процес передавання голосу через IPмережу проходить так:

Голос спершу оцифровується.

Оцифровані дані обробляються: видаляються паузи та шум, а також застосовується стиснення.

Оброблені дані розбиваються на пакети з інформацією про адресата, порядковим номером (для відновлення послідовності) і додатковими даними для корекції помилок.

Перш ніж пакет голосових даних потрапляє в мережу, ці дані тимчасово накопичуються, щоби сформувати повноцінний пакет для передачі. Аналогічно, при отриманні даних відбувається кілька етапів їх обробки (див. рис. 1.3).

Коли пакети з голосовими даними прибувають на сторону отримувача, система перевіряє їхню правильну послідовність. Через те, що IP-мережі не гарантують точний час доставки, можливі ситуації, коли пакети приходять у неправильному порядку або з різними затримками. Щоб відновити вихідну послідовність, дані тимчасово буферизуються (накопичуються). Проте окремі пакети можуть взагалі не дійти до одержувача або їх доставка буде занадто пізньою.

Оскільки передача голосу чутлива до затримок, повторна передача втрачених пакетів зазвичай не виконується. Замість цього застосовуються алгоритми відновлення — вони намагаються реконструювати відсутню інформацію за допомогою даних з наявних пакетів. Якщо це неможливо, пропуски можуть просто заміщуватися випадковими значеннями. Після цього отримана послідовність декомпресується і перетворюється на звуковий сигнал, який чує користувач.

Через буферизацію й часткові втрати даних якість відтвореного звуку може відрізнятися від оригіналу — як за точністю, так і за часом передачі. Тим не менш, людське вухо здатне сприймати мову навіть при часткових спотвореннях, що дозволяє користуватись IP-телефонією досить ефективно.

На сьогодні існує два основні способи передачі голосових пакетів через IP:

через загальнодоступний Інтернет;

через виділені корпоративні мережі на базі IP.

У першому випадку швидкість передачі залежить від навантаження в мережі, тому затримки можуть варіюватися. У випадку ж з виділеними каналами, які використовуються лише для голосу, можна забезпечити стабільну пропускну здатність і передбачувану затримку.

Хоча Інтернет є найпоширенішим каналом для IP-телефонії, варто зазначити, що у такому випадку провайдери не можуть гарантувати якість зв’язку.

Щоб здійснювати міжнародні або міжміські дзвінки через IP, провайдер має розміщувати телефонні сервери в регіонах, з яких і до яких здійснюються дзвінки. Завдяки цьому вартість таких розмов істотно менша, ніж у традиційній телефонії —

особливо це відчутно для міжнародних з'єднань.

1.2 Основні характеристики IP-телефонії

Принцип роботи телефонних серверів IP-телефонії такий: з одного боку сервер з’єднаний із традиційними телефонними лініями, з іншого — з мережею Інтернет. Він приймає аналоговий чи цифровий голосовий сигнал, стискає його, розбиває на пакети та надсилає через IP-мережу. Для зворотного напрямку — із мережі до телефонної лінії — процес виконується у зворотному порядку. Обидва процеси відбуваються практично одночасно, забезпечуючи можливість повноцінного двостороннього спілкування.

На основі цього принципу можна реалізувати різні типи зв’язку: наприклад, «телефон-комп’ютер» або «комп’ютер-телефон» — через один сервер, а для з’єднань типу «телефон-телефон» потрібні два сервери, кожен з яких працює зі своєю телефонною мережею.

Однією з головних перепон для масового впровадження IP-телефонії є те, що сам протокол IP не має вбудованих механізмів для гарантування якості обслуговування. Тому трапляються проблеми на кшталт спотворення звуку або його обривів, що особливо помітно в загальнодоступних мережах.

У приватних корпоративних мережах допустимий рівень втрат можна вважати прийнятним, якщо в середньому зв'язок залишається задовільним. Однак у відкритих мережах ситуація набагато складніша.

Незважаючи на технічні недоліки, IP-телефонія має величезний потенціал для масштабування — якщо не враховувати ризики погіршення якості при високому навантаженні, вона вже сьогодні є практичним і економічно вигідним рішенням.

Однією з головних переваг IP-зв’язку є те, що з’єднання на основі IP-протоколу може бути встановлено та завершено в будь-якій точці мережі — від окремого користувача до магістрального сегмента. Це дозволяє поетапно впроваджувати IP-телефонію в існуючу інфраструктуру — незалежно від того, чи йде мова про поступове оновлення зверху вниз, знизу вгору або за будь-якою іншою логікою. Системи IP-телефонії побудовані за модульним принципом: кількість шлюзів, gatekeeper-серверів (тобто систем керування номерними планами у VoIP) та інших вузлів можна збільшувати окремо, орієнтуючись на реальні потреби в навантаженні. При цьому розширення власне мережевої інфраструктури не є критичною умовою, адже самі IP-вузли можуть як взаємодіяти з телефонією, так і працювати автономно.

Попри численні прогнози, можна з упевненістю сказати: IP-телефонія ще не готова повністю витіснити класичну телефонію. Проте вона вже зараз може зайняти важливу нішу, насамперед у корпоративному середовищі. Тут особливо цінується можливість

паралельно передавати як голос, так і цифрові дані в одному каналі зв’язку. Це відкриває шлях для ефективного використання IP-телефонії у спільній роботі над документами, відеозустрічах, електронній комерції тощо. Навіть якщо якість мовлення не буде ідеальною, основне інформаційне навантаження часто несе текст або зображення на екрані комп’ютера, тож голос відіграє другорядну роль.

Таким чином, IP-телефонія стає важливою складовою сучасних мультимедійних систем, які поєднують оперативність, зручність та економічність використання мережевих ресурсів. У цьому контексті вона виступає як доповнення до інших каналів комунікації — передачі відео, файлів, веб-ресурсів тощо.

1.4 Основні моделі використання IP-телефонії

Оскільки IP-технології не вимагають фіксованих кінцевих пристроїв, користувачами можуть бути як звичайні телефони, підключені до телефонної мережі загального користування (ТМЗК), так і комп’ютери з відповідним програмним забезпеченням. Відповідно, виділяють три типові варіанти використання IP-телефонії:

зв’язок між двома комп’ютерами;

з’єднання між комп’ютером і телефоном;

дзвінки з телефону на телефон.

Найбільший інтерес з точки зору ефективності демонструють перші два варіанти — "комп’ютер-комп’ютер" та "комп’ютер-телефон", оскільки вони дозволяють одночасно передавати як голос, так і цифрові дані без втрат для операторів традиційного зв’язку.

У сценарії "комп’ютер-комп’ютер" застосовуються звичайні ПК з мультимедійними можливостями, підключені до інтернету. Аналоговий голос, що надходить до мікрофона, оцифровується, стискається за допомогою кодека (наприклад, із коефіцієнтами 4:1, 8:1 або 10:1), обгортається в IP-пакети з заголовками протоколів і передається через мережу. На приймаючій стороні все відбувається у зворотному порядку: розпакування, декомпресія, цифро-аналогове перетворення — і голос подається на динамік.

Для того щоб цей сценарій працював коректно, провайдер інтернету зазвичай використовує окремий сервер — gatekeeper — який відповідає за трансляцію імен користувачів у їхні IP-адреси. Як приклад програмного забезпечення можна навести Microsoft NetMeeting.

У другому сценарії — "комп’ютер-телефон" — найчастіше IP-з’єднання використовується для підтримки клієнтів: у службах технічної допомоги, консультацій або онлайн-

продажу. Користувач, що відвідує сайт компанії, може натиснути на кнопку зв’язку, після чого система автоматично з’єднає його з оператором, який користується звичайним телефонним апаратом.

Тут можливі два варіанти напрямку ініціації з’єднання:

користувач IP-мережі телефонує на ТМЗК;

або, навпаки, абонент ТМЗК ініціює дзвінок до користувача інтернету.

У першому випадку клієнт, перебуваючи в інтернеті, ініціює з’єднання з абонентом класичної телефонної мережі. Взаємодія мереж IP та ТМЗК відбувається через спеціальний шлюз, який може бути реалізований як окремий пристрій або інтегрований у наявну інфраструктуру.

У другому варіанті все навпаки — абонент ТМЗК набирає номер, а система спрямовує виклик до IP-мережі, де вже працює потрібний користувач.

1.3 Гнучкість розгортання та модульність IP-телефонії

Однією з ключових переваг IP-телефонії є можливість ініціації та завершення з’єднання в будь-якій точці мережі — від кінцевого абонента до магістрального сегменту. Це дозволяє впроваджувати систему поступово, сегмент за сегментом, що є особливо зручним під час міграції з традиційних систем. Перехід може здійснюватися як «зверху вниз», так і в зворотному напрямку чи за будь-якою іншою зручною схемою.

Системи IP-телефонії характеризуються високою модульністю: компоненти, такі як шлюзи або gatekeeper'и (сервіси керування номерними планами), можуть масштабуватися незалежно один від одного, залежно від поточних потреб. При цьому не враховуються можливі обмеження самої мережевої інфраструктури, оскільки її вузли можуть як бути частиною системи IP-телефонії, так і залишатися окремими.

Попри динамічний розвиток, наразі IP-телефонія не здатна повністю замінити традиційні телефонні системи. Проте в корпоративному секторі вона вже демонструє значну ефективність, забезпечуючи передачу голосу разом з даними в одному каналі зв’язку. Така інтеграція особливо корисна під час колективної роботи з інформацією, проведення відеоконференцій, онлайн-комерції та інших мультимедійних задач. Навіть за умов дещо нижчої якості голосу, ключову роль відіграє контекст інформації на екрані користувача, що компенсує вади голосового каналу.

Завдяки цьому IP-телефонія виконує роль додаткового засобу комунікації, який ефективно доповнює передачу даних, відео та веб-контенту, забезпечуючи гнучке мультимедійне середовище для сучасного бізнесу.

1.4 Основні сценарії використання IP-телефонії

IP-телефонія не обмежується типом кінцевого обладнання: у ній можуть використовуватись як звичайні телефони, підключені до традиційної телефонної мережі (ТМЗК), так і комп'ютери з відповідним програмним забезпеченням. Найбільш поширеними сценаріями є:

Комп'ютер – комп'ютер

Комп'ютер – телефон

Телефон – телефон

Сценарій «Комп'ютер – комп'ютер»

Реалізується між двома комп'ютерами, оснащеними мультимедійними засобами і підключеними до Інтернету. Аналоговий голосовий сигнал оцифровується за допомогою АЦП (аналогово-цифрового перетворювача), стискається за допомогою кодека (4:1, 8:1 або 10:1), пакується у формати IP-протоколів і передається через мережу. На приймальному боці дані декодуються, розпаковуються, проходять ЦАП і відтворюються у вигляді звуку.

Для такого з'єднання кожна сторона виконує одночасно функції передавання та прийому голосу. З метою адресації користувачів IP-мережі застосовується сервер gatekeeper, що транслює імена у динамічні IP-адреси. Найбільш поширеним клієнтським ПЗ свого часу був Microsoft NetMeeting.

Сценарій «Комп'ютер – телефон»

Цей варіант широко застосовується в службах підтримки, онлайн-продажах і довідкових системах. У рамках цього сценарію можливі два напрямки виклику:

від користувача IP-мережі до абонента ТМЗК;

від абонента ТМЗК до користувача IP-мережі.

2 ОГЛЯД ПРОТОКОЛІВ IP-ТЕЛЕФОНІЇ

2.1 Побудова мережі за рекомендацією H.323

У першому випадку користувач, відвідавши вебсайт, може ініціювати виклик до оператора через шлюз, що зв'язує IP-мережу з ТМЗК. У другому – ініціатором виступає користувач ТМЗК, а з'єднання надалі передається до IP-мережі через відповідний шлюз.

Сценарій «Телефон – телефон»

Цей сценарій має найбільше соціальне значення, оскільки дозволяє звичайним користувачам ТМЗК отримати альтернативу традиційному міжнародному та міжміському зв’язку, використовуючи IP-канал. У цьому випадку система IP-телефонії виконує роль віртуального каналу телефонного зв’язку.

2.1 Архітектура мережі H.323

Основною функцією шлюзу у мережі H.323 є трансформація мовного сигналу, що надходить зі сторони традиційної телефонної мережі (ТМЗК), у формат, придатний для передавання через пакетні IP-мережі. Додатково шлюз виконує перетворення сигналізаційних повідомлень, відповідно до стандартів DSS1 і ЗКС7, у сигнали протоколу H.323 та навпаки, згідно з рекомендацією ITU-T H.246.

Gatekeeper (реєстратор) виконує функції центрального інтелекту мережі IP-телефонії. В архітектурі H.323 використовується зональний підхід, згідно з яким мережа поділяється на зони (див. рисунок 2.2). Gatekeeper здійснює управління однією такою зоною, до якої входять зареєстровані термінали, шлюзи, пристрої керування конференціями тощо. Елементи зони можуть бути географічно розподіленими й поєднуватися між собою за допомогою маршрутизаторів.

До основних функцій gatekeeper належать:

реєстрація кінцевих пристроїв і мережевих компонентів;

контроль доступу до послуг IP-телефонії за допомогою сигналізації RAS;

трансляція alias-ідентифікаторів (ім’я користувача, номер телефону, електронна адреса тощо) у транспортні адреси (IP-адреса + TCP-порт);

управління пропускною здатністю мережі та її резервування;

ретрансляція сигналізаційних повідомлень H.323 між терміналами

У межах однієї IP-телефонної мережі може функціонувати декілька gatekeeper'ів, які взаємодіють між собою через протокол RAS. Крім базових функцій, gatekeeper також може забезпечувати автентифікацію користувачів та виконувати функції білінгу (нарахування плати за послуги зв’язку).

Пристрій керування конференціями забезпечує багатосторонній зв’язок між трьома або більше учасниками. У відповідності до рекомендації H.323, передбачено три типи конференцій:

Централізована – організовується за допомогою MCU (Multipoint Control Unit), де кожен учасник з'єднується з MCU у режимі "точка-точка";

Децентралізована – передбачає пряме з'єднання учасників один з одним у режимі "точка–група точок";

Змішана – поєднує елементи обох попередніх типів.

Перевагою централізованої конференції є відносна простота термінального обладнання, проте вона потребує дорогого спеціалізованого MCU. У децентралізованому варіанті, навпаки, потрібні більш складні термінали, а бажаною умовою є підтримка IP-мультирозсилки (multicast). Якщо така функція не підтримується, термінали змушені дублювати передачу голосових потоків до кожного учасника окремо.

MCU складається з обов’язкового контролера конференції (Multipoint Controller – MC) та, за необхідності, одного або кількох процесорів обробки даних (Multipoint Processor – MP). Контролер може бути інтегрований із gatekeeper, шлюзом або бути окремим пристроєм. Його функції включають узгодження режимів роботи учасників конференції, які можуть змінюватися динамічно, зокрема при підключенні нових учасників.

Оскільки в мережі може існувати кілька MCU, для кожної нової конференції необхідно виявити той контролер, який відповідатиме за її управління. У централізованих конференціях, крім MC, також використовується MP – він відповідає за перемикання або мікшування голосових, відео- та інших потоків. У децентралізованих конференціях MP, як правило, не потрібен.

Проксі-сервер H.323 та його Функції

Проксі-сервер H.323 — це ще один важливий компонент архітектури H.323. Він працює на прикладному рівні та виконує роль посередника між клієнтами. До основних функцій проксі-сервера належать:

Підключення терміналів: Забезпечує зв'язок терміналів через комутовані або локальні мережі, особливо якщо ці термінали не підтримують протокол RSVP (протокол резервування ресурсів).

Створення тунельних з'єднань: Формує тунелі з фіксованими параметрами якості обслуговування (QoS).

Маршрутизація H.323 трафіку: Керує маршрутизацією H.323 трафіку окремо від загального IP-трафіку.

Забезпечення сумісності з NAT: Дозволяє використовувати приватні IP-адреси завдяки сумісності з механізмами перетворення мережевих адрес (NAT). Обмеження доступу: Дозволяє доступ виключно для H.323-трафіку, що підвищує безпеку мережі.

Протоколи H.323: RAS, H.225.0, H.245

Протокол H.323 використовує кілька взаємопов'язаних протоколів для забезпечення своєї функціональності:

RAS (Registration, Admission, Status) Protocol: Цей протокол відповідає за взаємодію між кінцевими пристроями та gatekeeper. Його основні функції:

Реєстрація пристроїв у системі.

Контроль доступу до мережевих ресурсів.

Керування пропускною спроможністю в динамічному режимі.

Здійснення моніторингу стану пристроїв і передача актуальних даних. RAS базується на UDP для транспортування, що, незважаючи на відсутність гарантії доставки пакетів, забезпечує мінімальні затримки – ключовий фактор для якісної IP-телефонії.

H.225.0 (Q.931) Protocol: Регулює процеси ініціації, підтримки та припинення з'єднань. Для його функціонування застосовується TCP, що гарантує надійність з'єднання та доставку інформації.

H.245 Protocol: Призначений для обміну службовими даними між учасниками зв'язку. Ці дані критично важливі для формування логічних каналів, якими передається голосовий трафік у форматі RTP/UDP/IP-пакетів.

Сценарій Встановлення З'єднання в H.323

Процедури, що виконуються через протокол RAS, є першою фазою встановлення виклику згідно зі стандартом H.323. Після цього йде фаза сигналізації через H.225.0 (Q.931) та керуючий обмін повідомленнями через H.245. Завершення з'єднання відбувається у зворотному порядку: спочатку закривається керуючий канал H.245, потім сигнальний канал H.225.0, і лише після цього шлюз повідомляє gatekeeper через RAS про звільнення раніше зарезервованої смуги пропускання.

Типовий сценарій встановлення з'єднання виглядає наступним чином:

Кінцевий пристрій користувача А ініціює виклик, надсилаючи повідомлення SETUP до пристрою користувача Б через TCP-порт 1720.

У відповідь пристрій Б передає ALERTING, що означає готовність до виклику та сповіщення користувача про вхідний дзвінок.

Після прийняття виклику користувачем Б, пристрій надсилає CONNECT з інформацією про TCP-порт для H.245.

Далі по каналу H.245 відбувається обмін інформацією про використовувані кодеки (наприклад, G.729, G.723.1) та параметри з'єднання. Також передаються номери UDP-портів для голосового трафіку.

Потім встановлюються логічні канали, що забезпечують двосторонню передачу голосових даних за допомогою протоколу RTP. Одночасно, моніторинг якості цієї передачі виконується через RTCP.

Процедура "Швидкого Старту" та Додаткові Послуги H.323

Функція "швидкого старту" (Fast Start), інтегрована в H.323 версії 2, надає можливість включення даних для формування логічних каналів безпосередньо у повідомлення SETUP протоколу H.225.0, що дозволяє уникнути фази H.245. Це суттєво скорочує обсяг сигнального трафіку, необхідного для встановлення з'єднання.

Окрім основних можливостей, H.323 також підтримує надання розширених телекомунікаційних послуг, визначених у серії рекомендацій ITU-T H.450.X.

2.2 Мережі на Базі Протоколу SIP

Альтернативний підхід до IP-телефонії запропонувала робоча група MMUSIC IETF у документі RFC 2543. Цей протокол, відомий як SIP (Session Initiation Protocol), є текстовим і є частиною загальної мультимедійної архітектури IETF, яка також включає:

RSVP — для резервування ресурсів;

RTP — для передачі аудіо- та відеопотоків у реальному часі;

RTSP — для потокового мультимедіа;

SDP — для опису параметрів сесії.

SIP є незалежним від перелічених протоколів, хоча може працювати разом із ними.

Хоча SIP вважається легшим у впровадженні порівняно з H.323, його інтеграція з традиційними телефонними мережами (ТМЗК) є менш прямолінійною. Причина полягає в тому, що SIP використовує принципи HTTP, що ускладнює його сумісність з існуючими протоколами сигналізації ТМЗК. Отже, SIP оптимальніше підходить для

інтернет-провайдерів, які пропонують IP-телефонію як елемент ширшого пакету послуг.

Значною перевагою SIP є його здатність забезпечувати мобільність користувачів: абонент може користуватися послугами з будь-якого пристрою та місцезнаходження, при цьому мережа підтримує його ідентифікацію та автентифікацію під час переміщення.

Це досягається завдяки гнучкій системі адресації SIP, яка дозволяє використовувати такі формати адрес:

ім’я@домен;

ім’я@хост;

ім’я@IP-адреса;

номер_телефону@шлюз.

Таким чином, SIP-адреса завжди складається з двох частин: перша вказує на користувача, а друга — на домен чи пристрій, у якому він зареєстрований. Четвертий тип адреси є зручним для інтеграції з телефонними мережами.

Протокол SIP: Архітектура та Приклади Використання

Протокол SIP (Session Initiation Protocol) відіграє ключову роль у сучасних системах зв'язку, дозволяючи керувати мультимедійними сеансами: їх ініціюванням, модифікацією та завершенням. Його функціональність можна порівняти з іншими відомими протоколами, такими як HTTP або Mailto, що мають власні префікси ('http:', 'mailto:'). Для SIP цю роль виконує префікс 'sip:', який однозначно визначає адресу.

Приклади SIP-адрес:

sip:ost@imz.lviv.ua

sip:userl@192.168.1.152

sip:123-45-67@gateway.ua

Структура та Принципи Роботи SIP

Архітектура протоколу SIP тісно пов'язана з HTTP, базуючись на моделі "клієнт-сервер". У цій моделі, спілкування відбувається шляхом надсилання запитів від клієнта до сервера та отримання відповідей від сервера.

Структура SIP-Повідомлень

Кожне SIP-повідомлення має чітко визначену структуру:

Стартовий рядок: Містить ключову інформацію про повідомлення.

Заголовки: Включають службові дані, необхідні для обробки повідомлення.

Пустий рядок: Виконує роль роздільника між заголовками та тілом повідомлення.

Тіло повідомлення: Містить безпосередні дані сеансу.

Зміст стартового рядка залежить від типу повідомлення:

Для запиту він включає тип запиту, адресу призначення та версію протоколу.

Для відповіді — тип відповіді, її коротке пояснення та версію протоколу.

Заголовки ж надають детальні відомості, необхідні для коректної обробки конкретного повідомлення.

Деталізація SIP-Запиту на Прикладі INVITE

Розгляньмо значення ключових заголовків:

Via: Запобігає циклічному перенаправленню запиту в мережі.

From та To: Слугують для визначення ініціатора та цільового отримувача відповідно. Текст, що передує цим заголовкам, є іменем, яке відправник хоче показати на екрані отримувача.

Call-ID: Унікальний ідентифікатор певної сесії комунікації.

CSeq: Допомагає зіставляти запити з відповідями в рамках одного встановленого з'єднання.

Content-Type: Вказує формат, у якому представлено опис сеансу зв'язку.

Останній рядок містить відомості щодо протоколу та порту, що використовуються для передачі голосових даних, а також список підтримуваних кодеків (що представлені цифрами наприкінці рядка).

Основні Компоненти SIP-Мережі

SIP-мережа включає три ключові елементи, що забезпечують її функціонування:

Агент користувача (User Agent - UA): Це програмний компонент кінцевого пристрою, який має дві складові:

Агент користувача - клієнт (UAC): Створює та надсилає SIP-запити.

Агент користувача - сервер (UAS): Обробляє вхідні запити та формує відповіді.

Проксі-сервер (Proxy Server): Діє як посередник, поєднуючи функціональність клієнта та сервера, від імені інших клієнтів. Він здатен аналізувати та змінювати заголовки запитів перед їх подальшою передачею до інших серверів.

Сервер переадресації (Redirect Server): Визначає актуальне місцеположення абонента, що викликається, та передає ці дані ініціатору виклику, отримуючи інформацію від сервера локації.

Алгоритми Встановлення З'єднання SIP

Процес встановлення з'єднання за допомогою SIP може відбуватися з різною участю мережевих елементів.

Встановлення З'єднання Через Сервер Переадресації

Прийом запиту та визначення адреси: Сервер переадресації отримує запит INVITE від викличної сторони та зв'язується із сервером визначення місцезнаходження для отримання поточної адреси цільового користувача.

Передача адреси: Сервер переадресації передає знайдену адресу викличній стороні. Важливо відзначити, що, на відміну від проксі-сервера, сервер переадресації не здійснює пряму пересилку запиту INVITE до кінцевого пристрою абонента, що викликається. Замість цього, він надає викличній стороні необхідну адресу, після чого вже сам ініціатор виклику встановлює пряме з'єднання за отриманою адресою.

Підтвердження завершення транзакції: Обладнання викличного користувача підтверджує завершення взаємодії з сервером переадресації, відправляючи запит ACK.

Передача INVITE на отриману адресу: Далі, обладнання викличного користувача надсилає запит INVITE безпосередньо 1 на адресу, отриману від сервера переадресації.

1 Повідомлення про обробку: Пристрій абонента, що викликається, сповіщає 1 про вхідний виклик та надсилає викличному обладнанню інформацію (з кодом 100), яка вказує, 1 що запит INVITE перебуває в процесі обробки.

Завершення з'єднання: Коли адресат приймає виклик, ініціююче обладнання отримує відповідне підтвердження (з кодом 200). На цій стадії з'єднання є встановленим, і

абоненти можуть приступати до двостороннього голосового спілкування.

Типи Запитів у Протоколі SIP

Протокол SIP оперує шістьма основними типами запитів, кожен з яких виконує специфічну функцію. Система сигналізації SIP надає можливість користувацьким агентам та серверам мережі здійснювати визначення місцезнаходження, відправлення запитів та управління сеансами зв'язку.

INVITE: Цей запит слугує для початку участі користувача чи служби в комунікаційному сеансі, передаючи необхідні параметри. Він дозволяє абоненту визначити можливості обладнання партнера та швидко ініціювати сеанс, мінімізуючи кількість обмінів повідомленнями та підтвердженнями.

ACK: Запит ACK підтверджує успішне отримання 1 відповіді на команду INVITE, тим самим фіналізуючи поточну транзакцію.

OPTIONS: Запит OPTIONS використовується для отримання відомостей 1 про функціональні можливості користувацьких агентів та мережевих серверів, однак не 1 призначений для ініціювання 1 сеансів зв'язку.

1 BYE: Цей запит застосовується для припинення активного з'єднання між сторонами. Перед фактичним відключенням користувацькі агенти надсилають BYE-повідомлення серверу, інформуючи про бажання завершити сеанс.

CANCEL: Запит CANCEL 1 дає можливість користувацьким агентам та мережевим серверам анулювати раніше надісланий запит, у випадку, 1 якщо відповідь на нього ще не надійшла.

REGISTER: Клієнти використовують запит REGISTER для фіксації даних про своє місцезнаходження на SIP-серверах.

Мережі на Базі MGCP (Media Gateway Control Protocol)

Третій метод побудови IP-телефонії ґрунтується на застосуванні протоколу MGCP, розробленого робочою групою MEGACO під егідою IETF. Запропонована цією групою мережева архітектура включає три основні функціональні компоненти:

Шлюз (Media Gateway - MG): Здійснює конвертацію голосової інформації з традиційних телефонних мереж (ТМЗК), де вона передається зі сталою швидкістю, у формат для пакетної передачі по IP-мережах (що включає кодування та пакування голосу в пакети RTP/UDP/IP), а також виконує 1 зворотне перетворення.

1 Контролер шлюзів (Call Agent): Здійснює управління роботою шлюзів.

Шлюз сигналізації (Signaling Gateway - SG): Гарантує обмін сигнальною інформацією між ТМЗК та контролером шлюзів в обох напрямках.

В рамках цієї архітектури, вся інтелектуальна функціональність розподіленого шлюзу концентрується у контролері шлюзів, чиї можливості 1 можуть бути розподілені між різними 1 обчислювальними 1 платформами. Шлюз сигналізації функціонує як транзитний пункт (STP) для SS7-сигналізації, тоді як самі шлюзи відповідають виключно за перетворення голосових даних.

Єдиний контролер може керувати декількома шлюзами одночасно. Мережа може містити кілька контролерів, які, як правило, взаємно синхронізуються та спільно управляють шлюзами. Проте, протокол MEGACO не специфікує механізми для синхронізації між контролерами. Повідомлення MGCP передаються через UDP, що не забезпечує гарантованої доставки.

1 Шлюз сигналізації приймає пакети трьох нижніх рівнів системи сигналізації SS7 (рівнів підсистеми транспортування повідомлень, MTP) і ретранслює 1 сигнальні повідомлення верхнього, користувацького рівня до контролера шлюзів. Додатково, 1 шлюз сигналізації зобов'язаний передавати 1 сигнальні повідомлення Q-931 через IP-мережу.

Слід підкреслити, що MGCP є протоколом внутрішнього використання, призначеним для обміну даними між окремими функціональними компонентами розподіленого шлюзу, який зовні сприймається як цілісний пристрій. Контролер шлюзів виступає у ролі головного елемента, тоді як сам шлюз є підпорядкованим і мусить виконувати всі директиви.

Встановлення З'єднання Через Сервер Переадресації

Прийом та ідентифікація адреси: Сервер переадресації приймає запит INVITE від ініціатора виклику, після чого взаємодіє з сервером визначення місцезнаходження для отримання актуальної адреси цільового абонента.

Ретрансляція адреси: Сервер переадресації передає виявлену адресу абоненту-ініціатору. Важливо відзначити, що, на противагу проксі-серверу, сервер переадресації не пересилає запит INVITE напряму до пристрою викликаного абонента. Натомість, ініціююча сторона самостійно встановлює пряме з'єднання за отриманою адресою.

Підтвердження завершення операції: Пристрій, що ініціював виклик, підтверджує успішне завершення обміну даними з сервером переадресації, надсилаючи запит ACK.

Надсилання INVITE до цільової адреси: Після цього, пристрій ініціатора виклику безпосередньо відправляє 1 запит INVITE на адресу, отриману від сервера переадресації.

1 Повідомлення про обробку: Пристрій адресата інформує про вхідний дзвінок та надсилає пристрою-ініціатору повідомлення (код 100), вказуючи, 1 що запит INVITE обробляється.

1 Завершення встановлення зв'язку: Після того, як абонент, що викликається, приймає виклик, пристрій ініціатора отримує відповідне підтвердження (з кодом 200). На цьому етапі зв'язок вважається встановленим, і сторони можуть обмінюватися голосовими даними.

Типи Запитів у Протоколі SIP

Протокол SIP оперує шістьма основними типами запитів, кожен з яких виконує специфічну функцію. SIP-сигналізація дає змогу 1 користувацьким агентам і мережевим серверам визначати локацію, ініціювати запити та контролювати комунікаційні сесії.

INVITE: Цей запит ініціює залучення користувача або сервісу до сеансу комунікації, передаючи його основні параметри. Він дозволяє користувачеві виявити можливості терміналу співрозмовника та розпочати сесію з оптимальною кількістю сигнальних 1 повідомлень і підтверджень.

1 ACK: Запит ACK служить для підтвердження отримання 1 відповіді на команду INVITE, завершуючи таким чином поточну операцію.

OPTIONS: Запит OPTIONS використовується для отримання відомостей 1 про функціональні можливості користувацьких агентів та мережевих серверів, але не призначений для встановлення комунікаційних сеансів.

BYE: Цей запит застосовується учасниками для припинення активного 1 з'єднання. Перед тим як розірвати 1 зв'язок, 1 користувацькі агенти відправляють BYE серверу, інформуючи про своє бажання завершити сесію.

CANCEL: Запит CANCEL дає можливість користувацьким агентам та мережевим серверам анулювати попередньо надісланий запит, у разі, 1 якщо відповідь на нього ще не надійшла.

REGISTER: Клієнти використовують запит REGISTER для фіксації своїх даних про місцезнаходження на SIP-серверах.

Мережі на Базі MGCP (Media Gateway Control Protocol)

1 Третій підхід до організації IP-телефонії ґрунтується на застосуванні протоколу MGCP, розробленого робочою групою MEGACO під егідою IETF. Архітектура мережі, запропонована цим об'єднанням, включає три 1 основні функціональні блоки:

1 Шлюз (Media Gateway - MG): Призначений для конвертації голосових даних з традиційних телефонних мереж (ТМЗК) зі стабільною швидкістю потоку в формат, що підходить для пакетної передачі через IP-мережі (шляхом кодування та інкапсуляції голосу в пакети RTP/UDP/IP), а також виконує 1 зворотне перетворення.

1 Контролер шлюзів (Call Agent): Здійснює управління роботою шлюзів.

Шлюз сигналізації (Signaling Gateway - SG): Гарантує передачу сигнальних даних з 1 ТМЗК до контролера шлюзів, а також зворотну транспортування.

У цій архітектурі вся логіка розподіленого шлюзу концентрується в контролері шлюзів, чиї функції 1 можуть бути розподілені між різними комп'ютерними системами. Шлюз сигналізації виступає в ролі точки транзиту (STP) для сигналізації SS7. Самі ж шлюзи займаються виключно конвертацією голосових даних.

Єдиний контролер може одночасно керувати кількома шлюзами. Мережа може містити кілька контролерів, що, імовірно, координують свої дії та спільно керують шлюзами. Проте, протокол MEGACO не включає в себе механізмів синхронізації між контролерами. Повідомлення MGCP передаються через протокол UDP, який не забезпечує гарантованої доставки.

1 Шлюз сигналізації приймає пакети нижніх 1 трьох рівнів сигналізаційної системи SS7 1 (рівнів підсистеми переносу повідомлень MTP) 1 та ретранслює 1 сигнальні повідомлення верхнього, користувацького рівня до контролера шлюзів. Додатково, 1 шлюз сигналізації зобов'язаний передавати 1 сигнальні повідомлення Q-931 через IP-мережу.

Ось переглянутий текст з усуненим плагіатом та перефразованими розділами, на основі наданих зображень:

Слід підкреслити, що MGCP 1 є внутрішнім протоколом, призначеним 3 для обміну інформацією між окремими функціональними компонентами 1 розподіленого шлюзу, що зовні сприймається як єдиний пристрій. Контролер шлюзів виконує функцію основного керуючого елемента, тоді як сам шлюз є підпорядкованим і мусить дотримуватися всіх директив, отриманих 1 від контролера (Call Agent).

1 Додаткові послуги: Підтримка таких функцій, як переадресація викликів, конференц-

зв'язок тощо. Ці критерії дозволяють оцінити протоколи як з точки зору їх проектування та експлуатації, так і з позиції їх використання кінцевим користувачем.

3.1 Масштабованість Мережі

H.323: Мережі, побудовані відповідно до рекомендацій H.323, характеризуються зоновою архітектурою. Кожен gatekeeper адмініструє власну зону, що включає зареєстровані в ньому термінали, шлюзи та засоби управління конференціями. Окремі частини мережі H.323 можуть знаходитися в різних географічних місцях і поєднуються через маршрутизатори.

SIP: Мережі, що функціонують на протоколі SIP, демонструють масштабованість, аналогічну мережам H.323. Проте, ключова відмінність 3 полягає в тому, що SIP-сервер не обов'язково зберігає інформацію про активні з'єднання, що відрізняє його від gatekeeper H.323. Ця особливість сприяє обробці значно більшого обсягу вхідних викликів.

3.2 Розширюваність Протоколу

Забезпечення сумісності між різними версіями протоколів має першочергове значення. Розширюваність протоколу досягається завдяки:

Узгодженню параметрів

Стандартизації кодеків

Модульності архітектури

H.323: Нові функції інтегруються в протокол H.323 за допомогою поля Non Standard Parameter. Це поле включає код виробника, за яким слідує код послуги, дійсний лише для продукції цього виробника. Хоча такий підхід забезпечує певну можливість розширення послуг, він створює труднощі: по-перше, запит інформації про підтримку конкретних послуг є неможливим; по-друге, додавання нових значень до існуючих параметрів ускладнене. Крім того, виникають проблеми з сумісністю обладнання від різних виробників.

У протоколі H.323 необхідна стандартизація всіх кодеків. Це означає, що використання додатків з нестандартними алгоритмами кодування може призвести до складнощів при реалізації на платформі H.323.

Архітектура H.323 є монолітною, оскільки вона представлена як інтегрований набір протоколів, призначений для одного типу застосування. Вона складається з трьох ключових компонентів, і для впровадження нових послуг може виникнути потреба в

модифікації кожної з них.

SIP: Протокол SIP демонструє високу сумісність між різними версіями. Якщо пристрій розпізнає значення певного поля, то воно обробляється; нерозпізнані поля просто ігноруються. Це робить протокол простішим, спрощує обробку повідомлень та інтеграцію нових послуг. Для обміну інформацією про функціональні можливості терміналу в SIP застосовується протокол SDP.

Управління кодеками в SIP є значно простішим, ніж в H.323. Якщо виробник пропонує унікальний алгоритм кодування, достатньо його реєстрації в IANA.

Протокол SIP має модульну структуру, що дозволяє замінювати компоненти відповідно до потреб і забезпечувати їхнє незалежне функціонування.

MGCP: Загалом, розширення функціональності протоколу MGCP схоже на можливості SIP. Це зумовлено тим, що обидва протоколи застосовують ідентичний синтаксис для опису сеансів зв'язку — протокол SDP.

3.3 Підтримка Сигналізації ТМЗК

Підтримка сигналізації традиційних телефонних мереж (ТМЗК) залишається важливою. IP-мережа, що не дозволяє встановлювати з'єднання з абонентами ТМЗК, вважається неповноцінною.

H.323: Мережа, розроблена на основі рекомендацій H.323, досить схожа на традиційну телефонну мережу, і її можна сприймати як ISDN-мережу, що функціонує поверх IP. Однак слід зауважити, що в ранніх версіях протоколу сигналізація ТМЗК не передається прозоро, вимагаючи попередньої конвертації шлюзами в сигнальні повідомлення H.225.0.

SIP: Інтеграція SIP-мереж з традиційними телефонними мережами менш ефективна порівняно з іншими. У цьому сценарії, подібно до H.323, сигнальні повідомлення ТМЗК повинні бути перетворені шлюзами у формат SIP.

MGCP: Суттєвою перевагою протоколу MGCP є можливість підтримки контролером шлюзів (Call Agent) сигналізації ОКС-7 (SS7) та інших типів сигналізації, а також забезпечення прозорої передачі сигнальної інформації через IP-телефонію.

3.4 Час Встановлення З'єднання

H.323: Для встановлення з'єднання між абонентами за допомогою протоколу H.323 кінцеві термінали повинні обмінятися мінімум десятьма повідомленнями. Спочатку термінал запитує дозвіл у gatekeeper на використання мережевих ресурсів через

1 протокол RAS. Потім 1 між терміналами відбувається обмін керуючими повідомленнями, визначеними 1 в рекомендації H.225.0. Завершальним етапом 1 є обмін повідомленнями H.245, що дозволяють контролювати інформаційні канали. Цей процес 1 встановлення з'єднання є досить тривалим, що становить істотний недолік H.323.

Ось переглянутий текст з усуненим плагіатом та перефразованими розділами, на основі наданих зображень:

1 SIP: На відміну від H.323, 1 у 1 протоколі SIP для встановлення з'єднання потрібна лише одна транзакція. Запит 1 INVITE містить усю необхідну інформацію 1 для встановлення з'єднання, включно з описом 4 функціональних можливостей терміналу. 1 Крім того, SIP може використовувати механізм багатоадресної розсилки повідомлень для пошуку абонента за декількома зареєстрованими адресами, що значно прискорює встановлення з'єднання. 4 З цих причин час, витрачений 1 на встановлення з'єднання в протоколі SIP, значно менший, ніж у H.323. 4 Проте, 1 при використанні інкапсуляції повідомлень H.245 у повідомлення H.225 4 або 1 процедури Fast Connect, час встановлення з'єднання за допомогою протоколу H.323 суттєво зменшується.

Ось виправлений текст із перефразованими ділянками, що були позначені як плагіат:

1 Крім того, на швидкість встановлення з'єднання також впливає тип транспортного протоколу, задіяного для сигналізації. Початкові версії H.323 використовували виключно TCP для сигнальних повідомлень H.225 і H.245, тоді як лише з третьої версії була додана підтримка UDP. Протокол SIP, навпаки, від самого початку підтримує як TCP, так і UDP.

1 Час встановлення з'єднання вимірюється в умовних одиницях RTT (round trip time). Для SIP цей показник зазвичай становить 1.5 - 2.5 RTT, тоді як для H.323 він істотно вищий – 1 6-7 RTT.

1 MGCP: Щодо часу встановлення з'єднання з MGCP, важливо враховувати, що цей протокол розроблений лише для внутрішньої взаємодії між шлюзами та керуючими пристроями. Він не передбачає встановлення зв'язку між кінцевими терміналами. Таким чином, у цьому контексті, термін "час встановлення з'єднання" відноситься до портів шлюзів.

Для ініціації з'єднання в протоколі MGCP достатньо однієї команди – CRCX (Create Connection). Інші команди використовуються для зміни стану або розірвання з'єднання, управління портами та відповіді на події. З огляду на спеціалізоване призначення MGCP, час встановлення з'єднання між портами шлюзів є мінімальним.

3.5 Складність Протоколу

H.323: Протокол H.323, безумовно, є більш складним порівняно з SIP. Для встановлення з'єднання в H.323 задіяні три окремі протоколи (RAS, H.225, H.245), кожен з яких має власний набір повідомлень. H.323 працює з великою кількістю інформаційних полів у своїх повідомленнях, тоді як SIP має значно менше полів. H.323 використовує бінарний формат повідомлень, що ускладнює їх читабельність, незважаючи на швидшу обробку.

SIP: Для базового встановлення з'єднання в протоколі SIP достатньо трьох типів запитів: INVITE, BYE та ACK. SIP використовує текстовий формат повідомлень, аналогічно HTTP. Це суттєво спрощує синтаксичний аналіз, дозволяє введення даних вручну та загальний аналіз повідомлень.

MGCP: З точки зору складності, протокол MGCP схожий на SIP. Він також оперує текстовим форматом команд.

3.6 Адресація

H.323: Протокол H.323 використовує як транспортні, так і alias-адреси. Alias-адресами можуть бути телефонні номери, імена користувачів або електронні пошти. Конвертація alias-адрес у транспортні потребує залучення gatekeeper.

SIP: Використання URL є значною перевагою SIP. Це сприяє легкій інтеграції з існуючими DNS-системами та впровадженню в IP-сумісне обладнання. Адреса в SIP також може включати телефонний номер разом з адресою задіяного шлюзу.

3.7 Персональна Мобільність Користувачів

SIP: Протокол SIP має ефективні механізми для підтримки персональної мобільності абонентів. Користувачі SIP-мереж можуть реєструвати декілька адрес та встановлювати пріоритети для них. Це дозволяє здійснювати одночасний пошук користувача за кількома напрямками. При підключенні до мережі кожен кінцевий термінал реєструється на сервері визначення місцеположення, що забезпечує швидке виявлення поточної адреси користувача.

H.323: Персональна мобільність також підтримується H.323, проте вона менш гнучка. Наприклад, одночасний пошук користувача за декількома напрямками обмежений тим, що gatekeeper, отримавши запит на визначення місцезнаходження, не перенаправляє його до інших gatekeeper.

3.8 Додаткові Послуги

H.323: Додаткові послуги, доступні в протоколі H.323, стандартизовані в серії рекомендацій ITU-T H.450.X.

2 Приклади послуг, що надаються обома протоколами (H.323 та SIP):

2 Переключення з'єднання в режим утримання (Call hold);

2 Переключення зв'язку (Call Transfer);

2 Переадресація (Call Forwarding);

2 Повідомлення про новий виклик під час зв'язку (Call Waiting);

2 Конференція.

2 H.323: Рекомендація H.323 визначає три методи організації конференцій. Однак, 2 недоліком є те, що управління конференціями завжди централізоване — через контролер конференцій MC (Multipoint Controller). Отже, для проведення конференції, по-перше, потрібна наявність контролера MC у 2 одного з терміналів; по-друге, учасник з активним MC 2 не може залишити конференцію. 2 Крім того, при великій 2 кількості учасників MC 2 може стати "вузьким місцем". Перевагою H.323 у цьому аспекті є потужніші механізми контролю конференцій. H.323 забезпечує широкі можливості управління послугами, включаючи аутентифікацію, облік та контроль використання мережевих ресурсів. Можливості 2 SIP у цій сфері є менш розвиненими.

Нижче наведено переглянутий текст, у якому усунено плагіат і перефразовано виділені ділянки, згідно з наданими зображеннями:

2 SIP: Правила надання додаткових послуг у протоколі SIP не стандартизовані, що є значним недоліком. Це ускладнює організацію взаємодії між обладнанням різних виробників.

Протокол SIP підтримує три основні методи організації конференцій:

Використання пристроїв 2 керування конференціями (MCU).

2 Режим багатоадресної розсилки.

2 Режим з'єднання учасників один з одним.

2 У випадках багатоадресної розсилки та прямого з'єднання, управління конференціями може розподілятися між терміналами, що виключає необхідність централізованого контролера конференцій. Додатково, SIP дозволяє організовувати зв'язок за участі третьої сторони (third-party call control). Хоча H.323 також підтримує подібну послугу, її впровадження є значно складнішим.

4 ПРОЄКТУВАННЯ КОМПЛЕКСНОЇ СИСТЕМИ ІНТЕРНЕТ-ТЕЛЕФОНІЇ

4.1 Структура вузла віддаленого переговорного пункту

Структурно мережа складається з двох частин мережі центрального вузла, який являє собою вузол інтернет-провайдера з підтримкою передавання голосового трафіку та мережі віддалених переговорних пунктів.

На переговорному пункті міститься 12 кабін з телефонними апаратами. Апарати під’єднанні до FXS портів IP-шлюзів DYNAMIX DW 0004S по чотири на кожен. Для з'єднання апаратного забезпечення переговорного пункту використовується 16-портовий комутатор D-Link DES - 1016D з авто визначенням 10/100 BASE TX. У комутатор включено і систему білінгу, яка веде облік тарифікації розмов, використовуючи керуючі команди протоколу SIP.

Для безпечного виходу в Інтернет в цій мережі використовується firewall з активованим PAT (Ports Address Translation) (рисунок 4.1). Така структура дає можливість використовувати для кожного переговорного пункту одну публічну IP-адресу.

Рисунок 4.1 - Захист мережі за допомогою firewall з активованим PAT

Зв'язок з головним офісом доцільно здійснювати через орендовані канали зв'язку великих Інтернет-провайдерів, на „останній милі” доцільно використовувати протокол PPPoE. Основна перевага методу PPPoE полягає у використанні двох широко розповсюджених стандартизованих мережних структур, якими є стек протоколів PPP і локальна мережа Ethernet, що вимагає мінімальних змін існуючої інфраструктури мережі доступу (устаткування, операційних систем і т.д.) визначає мінімальні витрати і мінімальний час розгортання нових широкосмугових мережних послуг. Зазначені фактори важливі як для операторів зв'язку і провайдерів мережних послуг, так і для користувачів. Ключовою перевагою способу PPPoE є спрощення багатокористувацької інсталяції ліній доступу xDSL: Протокол PPPoE ідеально підходить для малих і домашніх офісів. Розрахунок пропускної здатності каналу наведений у таблиці 4.1.

Таблиці 4.1-Розрахунок пропускної здатності каналу

Спосіб передавання голосу

Тип канального протоколу

Смуга пропускання (bps) (кодек G.711)

Смуга пропускання (bps) (кодек G.729)

Смуга пропускання (bps) (кодек G.723)

Digital

TDM

64 000

8 000

6 300

VoIP

802.3

84 800

28 800

27 200

VoIP

Ethernet

84 800

28 800

27 200

VoIP

Frame Relay

76 267

20 267

18 667

VoIP

PPP

76 800

20 800

19 200

VoIP

ATM(AAL-5)

84 800

28 267

28 267

VoIP/he

Frame Relay

66 933

10 933

9 933

VoIP/he

PPP

67 467

11467

9 867

VoFR/hc

Frame Relay

66 400

10400

8 800

VoATM/hc

ATM(AAL-5)

84 800

14 133

14 133

Експортувати в Таблиці

Розрахуємо пропускну здатність для двох кодеків G.729 та G.723 V(G.729) = 28 800* 12=365 600 біт/с; V(G.723) = 27 200*12=326 400 біт/с; Враховуючи тарифні плани Інтернет-провайдера доцільно вибрати канал з пропускною здатністю 512Кбіт/с. Що можливо при підтримці даної технології xDSL-модемом. Для даного з'єднання доцільно використати модем типу CT-500 - HSDSL модем/маршрутизатор, розроблений на чипсеті ADI, призначені для застосування в малих і середніх офісах чи для об'єднання віддалених офісів компаній. Має один Ethernet порт для підключення до мережі, забезпечує доступ в Internet, корпоративні мережі по звичайній телефонній лінії зі швидкістю до 2Мбіт/с (рис.4.2).

Рисунок 4.2 - Фронтальна панель CT-500

4.2 Обґрунтування вибору апаратної частини ISP

Центральний маршрутизатор вузла є основною компонентою, що пов'язує мережу Інтернет та користувачами Інтернет-вузла. Основними функціями, що повинен виконувати даний маршрутизатор є:

Зв'язок мережі інтернет-провайдера з мережею Інтернет

Передавання трафіку між різними компонентами вузла

Фільтрацію трафіку та попередження атак на вузол на первинному рівні

Регулювання смуги пропускання між клієнтами Інтернет-провайдера та мережею Інтернет

Регулювання смуги пропускання між клієнтами вузла і серверами застосувань

Регулювання смуги пропускання між серверами застосувань, web-hosting серверами та мережею Інтернет

Переадресація HTTP-трафіку в кеш-сервер

Для вирішення всіх перерахованих задач, вибираємо високопродуктивний маршрутизатор Access Point 1000. Access Point 1000 здатний комутувати до 200 тис. пакетів у секунду при включенні більшості опцій, у тому числі пакетних фільтрів і функцій контролю і керування якістю послуг (QoS). Access Point 1000 має повний набір стандартизованих опцій безпеки для створення VPN і підтримує до 4000 одночасно активних тунелів VPN. Його компактний розмір (усього 1.75 дюйма у висоту при

монтажі в 19" стійку) дозволяє оптимально використовувати місце в стійці, де встановлюється устаткування.

Базовий комплект (шасі) маршрутизатора Access Point 1000 містить два порти Ethernet 10/ЮОТХ і 4 слота для установки додаткових модулів. Для підключення до зовнішньої мережі можна використовувати кілька варіантів інтерфейсів - від порту V.35 на початковому етапі до високошвидкісного інтерфейсу ATM, що працює на швидкості 155Мбіт/з, при росту навантаження на вузол. При необхідності, у маршрутизатор можна установити наступні модулі:

• 4 порти E1

• 1 порт гігабітного Ethernet

• 1 порт HSSI чи MSSI (V.35)

Як сервери доступу використовуються пристрої серії MAX 6000 на схемі показано два: один з них забезпечує доступ до Інтернет користувачів по комутованих лініях, та доступ в Інтернет по виділеній лінії, а інший - доступ до послуг IP-телефонії та інших застосувань реального часу. При такому рішенні є можливість пере направити мультимедійний трафік по заздалегідь зарезервованих каналах з гарантованим QoS. Обидва сервери працюють під управлінням протоколу RADIUS.

Для доступу в Інтернет використовується MAX6060 із встановленими 60 цифровими модемами, що підтримують всі існуючі протоколи, включаючи V.90 і K56flex.. У шасі MAX6060 інтегровано чотири порти E1, які можна використовувати для підключення до телефонної мережі по ISDN PRI для організації dial-up і ISDN доступу, а також для підключення до TDM-мережі для організації доступу по виділених каналах. У такий спосіб до сервера може бути одночасно підключене до 96 користувачів доступу через комутовані лінії, або до 120 одночасно працюючих ISDN-клієнтів, або клієнтів, що використовують виділені лінії. Якщо телефонна станція, до якої підключається сервер доступу, не підтримує ISDN, можна використовувати сигналізацію R2.

Таким чином до Інтернет-вузла може бути підключено до 180 одночасно працюючих клієнтів комутованого доступу (120 з них за допомогою модемів, від 60 одночасно з модемами до 180 при відсутності модемних викликів з допомогою ISDN BRI) і до 60 виділених ліній. В останньому випадку загальна кількість виділених ліній може змінюватись в залежності від конкретних значень перепускної здатності кожної лінії.

Дане рішення є легко масштабується та є досить гнучке:

по-перше кількість модемів у кожному сервері може бути збільшено до 90 шляхом

простого додавання модулів цифрових модемів

по-друге кількість самих серверів доступу може бути збільшено без суттєвої зміни в інфраструктурі вузла

по третє при необхідності збільшення кількості клієнтів, що працюють по виділених лініях, можна встановити пусте шасі MAX 6000, що забезпечить додатково 4 порти E1, тобто можливість підключення до240 виділених ліній.

Для надійності кожен з серверів доступу обладнується двома блоками живлення, а також навантаження комутованих ліній може бути розподілене між кількома серверами доступу і у випадку відмови в роботі одного з них не відбудеться повної відмови сервісу, а тільки погіршаться характеристики продуктивності візлу (тобто зменшиться кількість успішних з'єднань).

Аналогічний пристрій використовується і для надання послуг IP-телефонії. Для цього необхідно установити на MAX 6000 спеціальну версію операційної системи TAOS з підтримкою можливостей передачі голосу по IP - MultiVoice і 12- або 16-портові модулі сигнальних процесорів (DSP). MultiVoice MAX 6000 можна оснастити DSP-модулями на 96 каналів. При цьому незайняті канали в підключених до нього потоках E1 можна використовувати для надання послуг по виділених лініях, або за допомогою ISDN.

Завдяки використанню єдиної платформи керування Navis Access гарантована зручність керування і контролю за послугами комутованого ISDN (IDSL) і модемного доступу по комутованих лініях, доступу по виділених лініях і IP-телефонії. Як диспетчера шлюзів IP телефонії (gatekeeper) використовується програмне забезпечення Multivoice Access Manager, що здійснює підтримку протоколу SIP, трансляцію телефонних номерів і авторизацію користувачів. Воно встановлено на спеціальному сервері, підключеному в сегмент службових серверів. Це може бути або стандартний PC-сервер під керуванням Windows NT, або сервер SUN під керуванням Solaris.

Для зниження навантаження на зовнішній канал зв'язку застосовується кеш-сервер. Крім своєї основної функції - зниження кількості зовнішніх запитів за рахунок усунення повторних звертань до тому самому ресурсу - він дозволяє надавати також додаткові послуги. Наприклад, він може працювати "у зворотну сторону" - зменшувати кількість повторних запитів до власних серверів провайдера і розташованим на його території серверам клієнтів і, таким чином, згладжувати піки активності користувачів.

Використовуваний кеш-сервер Lucent WebCache 100 має високу продуктивність - більш 500 запитів у секунду. Спеціальні алгоритми кешування, розроблені в Bell Labs, здатні заощадити до 70% пропускної здатності каналів зв'язку. Кеш-сервер здатний здійснювати захист від сплесків трафіку, забезпечувати гарантоване надання

визначеного рівня якості сервісу, надання тимчасових додаткових потужностей під час періодів пікового навантаження, а також> послуг по динамічній реплікації. Основними характеристиками даного сервера є:

Висока продуктивність — більше 500 запитів в секунду

Спеціальний алгоритм кешування, що здатний економити до 70% пропускної здатності каналів зв'язку

Легкість інтеграції з маршрутизатором Access Point 1000, який у "прозорому" для кінцевого користувача режимі перенаправляє всі HTTP- запити користувача на кеш-сервер. Тобто клієнтам навіть не мають необхідності проводити додаткове налаштування інтернет-браузера.

У якості між мережевого екрану встановлений Lucent Managed Firewall (LMF) -це комплекс, що складається з декількох компонентів:

LMF Brick, пристрій (блок) працює на рівні моста локальної мережі, і забезпечує аналіз, облік і, при необхідності, блокування трафіку, що через нього проходить. Блок працює під керуванням спеціальної операційної системи Inferno, розробленої в Bell Labs і має значно більшу продуктивністю у порівнянні з екранами, що працюють під управлінням ОС загального користування, таких як Windows NT і Solaris.

Security Management Server - сервер, що керує блоками (Brick). Адміністратор безпеки за допомогою сервера SMS може призначати і керувати політиками безпеки на всіх блоках у мережі.

Lucent Real Secure - сканер атак, що проводить аналіз трафіку і попереджуючий про спроби несанкціонованого доступу до мережі. Сканер Real Secure працює в непомітному для всієї мережі режимі і посилає попередження на консоль сервера SMS про всі спроби атак. Крім цього взаємодіючи з сервером SMS і блоками, сканер може переривати сесію, що може нести потенційну загрозу безпеки.

За допомогою між мережевого екрану організується безпека двох найбільш важливих елементів мережі: сегменту службових серверів (диспетчер шлюзів VoIP, RADIUS-сервер) і офісної локальної мережі. Крім того, забезпечується захист від можливих атак з офісної мережі, спрямованих на вузол телекомунікаційних послуг. Безпека серверів доступу, серверів-застосувань, кэш-сервера і системи моніторингу організована за допомогою фільтрів на центральному маршрутизаторі вузла. Для об'єднання устаткування, що входить у вузол доступу, використовується комутатор Cajun P333T, що має 24 порти 10/100BASE-TX. За допомогою даного пристрою усі компоненти, що входять у вузол доступу будуть рознесеш на 6 віртуальних локальних мереж (VLAN).

(Реально створюємо 8 IP-підмереж, але задіємо 6, а дві залишаємо в резерві). В окремий порт комутатора, а також і в окремий VLAN, передбачається включити центральний маршрутизатор вузла.

Основні Переваги Визначення VLAN на Рівні 3

Визначення VLAN на третьому (мережевому) рівні моделі OSI надає кілька суттєвих переваг, що робить його привабливим для адміністраторів мереж.

Розділення за типами протоколів: Цей підхід дозволяє створювати VLAN-и, орієнтовані на певні послуги або програми, базуючись на їхніх протоколах. Це особливо зручно для адміністраторів, які спеціалізуються на такій стратегії організації віртуальних мереж.

Гнучкість переміщення робочих станцій: Користувачі можуть фізично переміщати свої комп'ютери або інші мережеві пристрої без необхідності переналаштування їхніх IP-адрес. Ця перевага є особливо цінною для користувачів, що працюють з протоколом TCP/IP.

Зменшення мережевого навантаження: Визначення VLAN на Рівні 3 усуває потребу в спеціальних "позначках" (тегах) для мережевих кадрів під час обміну даними між комутаторами в межах одного VLAN. Це призводить до зменшення обсягу службової інформації, що передається мережею, і, відповідно, знижує загальне транспортне навантаження.

Оскільки і маршрутизатор, і комутатор підтримують специфікацію ШЕЕ 802.1Q передачі сигналізації VLAN, то маршрутизатор може здійснювати маршрутизацію і фільтрацію IP-пакетів між усіма - віртуальними мережами, -при цьому продуктивність маршрутизатора не погіршується, тому що інформація про VLAN-сигналізацію обробляється на рівні контролера Ethernet, і потім передається вже в обробленому виді в ядро маршрутизатора

Описана архітектура вузла має великі можливості для подальшого росту і розширення. Продуктивності основних його компонентів цілком достатньо для обслуговування великого Інтернет-вузла, а їхня невисока ціна дозволяє використовувати їх із самого початку надання послуг. Основним напрямком розширення є збільшення числа серверів доступу MAX 6000 для користувачів комутованих ліній, і VoIP-шлюзів MAX 6000 MultiVoice для розширення надання послуг IP-телефошї.

4.3 Поділ даної мережі на підмережі та визначення діапазону IP-адрес для проектованої мережі

IP-адреса має дворівневу структуру (рис 4.3)

Рисунок 4.3 - Загальна структура IP-адреси

Перша частина IP-адреси ідентифікує мережу, до якої під’єднана станція, а друга - конкретну станцію у даній мережі. Першу частину адреси називають номером мережі, ідентифікатором мережі (NetED) або, частіше, мережевим префіксом; другу частину - мережевим суфіксом, номером станції або ідентифікатором станції (HostID).

Для супроводу мереж різного розміру при повно класовій адресації IP-адреси, представлені 32-бітовим кодом, ділять на наперед задані класи класи: A, B, C, D, E. Практичне використання на даний час мають перші 3 класи: A, B і C. При повно класовій IP-адресації кожна адреса містить ключ само ідентифікації – перші зліва біти IP-адреси. Для ключа само ідентифікації адрес класу A використовують 1 біт (02), для адрес класу B - 2 біти (102), для адрес класу C - 3 біти (1102). Оскільки 32-бітову IP-адресу можна поділити на чотири 8-бітові поля (байти), то для спрощення запису і читання IP-адрес людьми IP-адреси часто виражають чотирма десятковими числами, розділеними крапками, тобто у формі у AAA.BBB.CCC.DDD. Кожне десяткове число виражає десяткове значення відповідного байта IP-адреси. Наприклад, для класу C маємо наступний перелік адрес (таблиця 4.2):

Таблиця 4.2. Діапазон IP-адрес для класу C.

Клас

Найменша адреса

Найбільша адреса

C

192.0.1.xxx

223.255.255.xxx

Кожна мережа, що зазвичай асоціюється з певною організаційною структурою (наприклад, фірмою, підприємством, установою), отримує частину адресного простору у вигляді одного або кількох блоків адрес зі спільним мережевим префіксом.

Суть ієрархічної організації підмереж у мережах класів A, B і C полягає в переході від дворівневої структури IP-адреси до трирівневої. Замість того, щоб IP-адреса складалася лише з мережевого префікса (NetID) та номера станції (HostID), початковий суфікс HostID поділяється на дві частини: адресу підмережі (SubNetID) та власне номер станції (HostID).

Кількість бітів, відведених для номера підмережі, визначається необхідною кількістю підмереж і завжди має бути цілим степенем 2. Наприклад, для 2 підмереж потрібен 1 біт (21=2), для 4 — 2 біти (22=4), для 8 — 3 біти (23=8), для 16 — 4 біти (24=16), і так далі. При плануванні мережі та врахуванні її майбутнього розширення, кількість підмереж завжди округлюється до найближчого більшого числа, яке є степенем 2. Це демонструє, як реалізується трирівнева ієрархія IP-адрес.

Кожна підмережа працює як самостійна локальна мережа. Зв'язок між підмережами вимагає таких же механізмів, як і зв'язок між повністю окремими мережами. Станції в різних підмережах не можуть безпосередньо взаємодіяти, якщо не передбачено спеціальних засобів для такого зв'язку.

В проектованій мережі використовується клас С Маємо наступний адрес мережі: 192.1.0.0. Перші 3 байти являють собою адресу мережі (класу С). Останні 8 біт призначені для визначення номера станції та номера підмережі. Потрібно створити 2 підмереж. Для цього нам потрібно 1 біт і на адресацію станцій залишається 7 біт, що дає змогу організувати по 27-2=126 комп'ютерів в підмережі. В проектованій мережі використовується клас С. Маємо наступний адрес мережі: 192.1.0.0.

Одна з мереж VLAN_1 призначена для обслуговування комутованих та користувачів виділених ліній. У цю мережу входить і сервер доступу MAX 6060. Для даної мережі виділяють IP адреси в діапазоні 192.1.0.129 -192.1.0.254. Все інше обладнання Інтернет-вузла входить у підмережі, які формуються з адрес, що залишились.

Для обслуговування користувачів IP-телефонії формують віртуальну мережу VLAN_2 у яку входить також і сервер доступу Multi Voice MAX 6000. Для цієї мережі відводимо діапазон адрес: 192.1.0.65 - 192.1.0.126. З адрес, що залишились формуємо чотири підмережі.

VLAN_3 до якої входять всі сервери застосувань і використовується діапазон адрес 192.1.0.1-192.1.0.14

VLAN_4 до якої входять засоби для управління та моніторингом Інтернет-провайдера і мають діапазон адрес 192.1.0.17- 192.1.0.30

VLAN_5 до якої входить кеш-сервери і використовується діапазон адрес 192.1.0.33 – 192.1.0.46

VLAN_6 до якої входять міжмережевий екран службові сервери і використовується діапазон адрес 192.1.0.49 – 192.1.0.62

Посилання

Це джерела виділених збігів у вашому документі. Кожен збіг позначено темно-зеленим числом, яке відповідає вказаному тут джерелу. Джерела впорядковані за схожістю — чим вищий бал, тим сильніше збіг.

#	Джерело	%
1	dut.edu.ua	3.7%
2	duikt.edu.ua	1.6%
3	repositsc.nuczu.edu.ua	0.1%
4	dspace.wunu.edu.ua	0.1%

Plag

Дякуємо, що перевірили
свій документ за допомогою
Plag!