

**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ**

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“ _____ ” _____ 2021 р.

**ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)**

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «iSC SI2000 в ролі шлюзу IP-мережі»_____.

Виконавець: _____ Христенко О.І.
(підпис)

Керівник: _____ Антонов В.В.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій

Кафедра телекомунікаційних та радіоелектронних систем

Спеціальність 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

Одарченко Р.С.

“ ” 2021 р.

ЗАВДАННЯ на виконання дипломної роботи

Христенку Олександрю Ігоровичу

(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): «iSC SI2000 в ролі шлюзу IP-мережі»

затверджена наказом ректора від «06» квітня 2021 р. №559/ст

2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.

3. Вихідні дані до роботи: методи побудови мережі IP, АТС, Asterisk, ISKRATEL SI2000, SIP, PRI.

4. Зміст пояснювальної записки:

- Розділ 1 «IP, IP-мережі, IP-телефонія та VoIP»
- Розділ 2 «VoIP обладнання, Asterisk та SI2000»
- Розділ 3 «Побудова каналу зв'язку між Asterisk та SI2000»

5. Перелік обов'язкового графічного (ілюстративного) матеріалу: Рис. 2.6

ISKRATEL SI2000 всередині, Рис.2.7 Блок-схема модуля MLC АТС SI-2000, Рис. 3.1

Приклад IP-шлюзу з з'єднанням в мережі TDM і IP, Рис. 3.2 Вхід до системи

управління, Рис. 3.19 Схема порядку створення вихідного маршруту, Рис. 3.34

Лістинг налаштувань з'єднувальної лінії, Рис. 3.35 Результат команди rasterisk -x 'sip

show peers', Рис. 3.36 Лістинг налаштувань маршрутизації

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021- 21.05.2021	Виконано
2	Вступ	21.05.2021- 23.05.2021	Виконано
3	IP, IP-мережі, IP-телефонія та VoIP	23.05.2021- 27.05.2021	Виконано
4	VoIP обладнання, Asterisk та SI2000	27.05.2021- 1.06.2021	Виконано
5	Побудова каналу зв'язку між Asterisk та SI2000	1.06.2021- 7.06.2021	Виконано
6	Усунення недоліків дипломної роботи	7.06.2021- 21.06.2021	Виконано

7. Дата видачі завдання: "26" квітня 2021 р.

Керівник дипломної роботи _____ Антонов В.В.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Христенко О.І.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «iSC SI2000 в ролі шлюзу IP-мережі» містить 68 сторінок, 44 рисунки, 1 таблицю, 15 використаних джерел.

Ключові слова: IP-ТЕЛЕФОНІЯ, ASTERISK, АТС, SI2000

Об'єкт дослідження – Побудова каналу зв'язку.

Предмет дослідження – Канал зв'язку між SI2000 та Asterisk.

Мета дипломної роботи – побудувати канал зв'язку між SI2000 та Asterisk.

Метод дослідження – порівняльний метод, статистичний аналіз, структурний аналіз, прийоми аналізу наукової літератури, порівняльний метод.

Матеріали дипломної роботи рекомендується використовувати при побудові каналу зв'язку між Asterisk та цифровою АТС, встановленні та налаштуванні Asterisk, а також при налаштуванні АТС ISKRATEL SI2000 або SI3000.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ	11
ВСТУП	12
РОЗДІЛ 1. IP, IP-мережі, IP-телефонія та VoIP.	14
1.1. Аналіз поняття IP та IP-мережа.....	14
1.2. IP-телефонія	18
1.3. VoIP.....	19
1.3. Протоколи VoIP..	20
Висновки до розділу 1.....	27
РОЗДІЛ 2. VoIP обладнання, Asterisk та SI2000.....	28
2.1. VoIP обладнання.....	28
2.2. Основні кодеки які використовуються в VoIP.....	32
2.3. Asterisk.....	36
2.4. ISKRATEL SI2000.....	37
Висновки до розділу 2.....	41
РОЗДІЛ 3. Побудова каналу зв'язку між Asterisk та SI2000.....	42
3.1. Конфігурування іCS з функціями IP-шлюзу	42
3.2. Налаштування маршрутизації SI2000.....	52
3.3. Встановлення та налаштування Asterisk 13.....	62
3.3.1. Встановлення Asterisk 13.....	62
3.3.2. Налаштування каналу зв'язку на Asterisk.....	63
3.3.3. Налаштування маршрутизації на Asterisk.....	64
Висновки до розділу 3.....	65
ВИСНОВКИ	66
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	68

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

iCS – Integrated Call Server
IP – Internet Protocol
VoIP – Voice over Inter Protocol
TCP – Transmission Control Protocol
UDP – User Datagram Protocol
LAN – Local Area Network
АТС – Автоматична телефонна станція
GSM – Groupe Spécial Mobile
ПЗ – Програмне забезпечення
PRI – Primary Rate Interface
SIP – Session Initiation Protocol
RTP – Real-time Transport Protocol
SS7 – Signaling System 7
DSS1 – Digital Subscriber System №1
TDM – Time-division multiplexing
PBX – Private Branch Exchange
PSTN – Public Switched Telephone Network
ATM – Asynchronous Transfer Mode
ISDN – Integrated Services Digital Network
IETF – Internet Engineering Task Force
HTTP – Hypertext Transfer Protocol
DNS – Domain Name System
CPU – Central Processing Unit
DDR – Double Data Rate
HDD – Hard Disk Drive

ВСТУП

Актуальність теми. На сьогоднішній день IP-телефонія як і будь яка сучасна технологія стрімко розвивається, але нові технології впроваджуються не так швидко як розвиваються. На підприємствах продовжують використовуватися аналогові та цифрові АТС завдяки своїм перевагам таким як можливість використання в важкодоступних місцях, що не входять в зону покриття стільникового зв'язку, незалежності від Інтернету та електропостачання, а також оскільки вони були придбані ще в часи коли IP-телефонія тільки починала свій розвиток. Але недоліки аналогової телефонії такі як низька якість переданого звуку, обмеженість функціоналу, а також необхідність в прокладанні окремих дорогих ліній для кожного номера змушують використовувати IP-АТС такі як Asterisk.

Додавання до такого комплексу телефонії IP-АТС дає можливість використовувати переваги обох технологій, з одного боку це стабільність, надійність та сумісність з застарілими технологіями, а з іншого боку висока якість зв'язку, мобільність, розширений функціонал, низька вартість передачі даних та простота експлуатації.

Мета і завдання дослідження. Мета дипломного проекту полягає в тому щоб розробити методологію підключення IP АТС Asterisk до цифрової АТС SI2000 та налаштування SI2000 в якості IP шлюза.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Аналіз літератури та методичних вказівок для налаштування АТС.
2. Налаштування iCS SI2000 в якості шлюза IP мережі.
3. Встановлення та налаштування Asterisk

Об'єктом дослідження – Побудова каналу зв'язку між цифровою АТС та IP АТС

Предметом дослідження – iCS SI2000 в якості шлюза IP мережі.

Методи досліджень. Для досягнення поставлених цілей в роботі використано: порівняльний метод, статистичний аналіз, структурний аналіз, прийоми аналізу наукової літератури, порівняльний метод.

Практичне значення отриманих результатів. Результати дипломного проекту можна використовувати при роботі з IP мережами, IP-телефонією, Asterisk та АТС SI2000.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2020 р.

РОЗДІЛ 1

IP, IP-МЕРЕЖІ, IP-ТЕЛЕФОНІЯ ТА VOIP

1.1. Аналіз поняття IP та IP-мережа

Internet Protocol (IP) - це протокол або набір правил для маршрутизації та адресації пакетів даних, що регулюють формат даних, що надсилаються через Інтернет або локальну мережу, щоб вони могли переміщуватися по мережі та прийти до потрібного місця призначення. Дані, що передаються через Інтернет, діляться на менші частини, які називаються пакетами. Інформація про IP додається до кожного пакету, і ця інформація допомагає маршрутизаторам направляти пакети в потрібне місце. Кожному пристрою або домену, що підключаються до Інтернету, присвоюється IP-адреса, і оскільки пакети перенаправляються на призначену їм IP-адресу, дані надходять туди куди потрібно.

Як тільки пакети надходять до місця призначення, вони обробляються по-різному, залежно від того, який транспортний протокол використовується разом з IP. Найпоширенішими транспортними протоколами є TCP та UDP.

IP-адреса - це унікальна адреса, яка ідентифікує пристрій в Інтернеті або локальній мережі. [2]

По суті, IP-адреси - це ідентифікатор, який дозволяє передавати інформацію між пристроями в мережі: вони містять інформацію про місцезнаходження та роблять пристрої доступними для спілкування. Інтернету потрібен спосіб розрізнити різні комп'ютери, маршрутизатори та веб-сайти. IP-адреси забезпечують цю можливість і становлять важливу частину того, як працює Інтернет. [2]

IP-адреса - це рядок чисел, розділених крапками. IP-адреси виражаються у вигляді набору з чотирьох чисел - прикладом може бути 192.158.1.38. Кожне

число в наборі може бути в діапазоні від 0 до 255. Отже, повний діапазон IP-адресації варіюється від 0.0.0.0 до 255.255.255.255. [2]

IP-адреси не є випадковими. Вони розподіляються Адміністрацією адресного простору Інтернет (IANA), підрозділом Інтернет-корпорації з присвоєння імен та номерів (ICANN). ICANN - це некомерційна організація, яка була створена в США в 1998 році, щоб допомогти підтримувати безпеку Інтернету та надати можливість використовувати Інтернет усім. Кожен раз, коли хтось реєструє домен в Інтернеті, вони проходять реєстратор доменних імен, який платить невелику плату ICANN за реєстрацію домену. [2]

Інтернет-протокол працює так само, як і будь-яка інша мова, спілкуючись за допомогою встановлених вказівок для передачі інформації. Усі пристрої знаходять, надсилають та обмінюються інформацією з іншими підключеними пристроями за допомогою цього протоколу. Розмовляючи однією мовою, будь-які комп'ютери у будь-якому місці можуть спілкуватися між собою. [2]

Процес відбувається таким чином:

1. Ваш пристрій підключається до Інтернету, спочатку підключившись до мережі, підключеної до Інтернету, яка надає Вашому пристрою доступ до Інтернету.
2. Коли ви будете вдома, ця мережа, ймовірно, буде вашим постачальником послуг Інтернету..
3. Ваша IP-адреса призначається вашому пристрою провайдером.
4. Ваша активність в Інтернеті проходить через Інтернет-провайдера, і вони направляють його назад вам, використовуючи вашу IP-адресу. Оскільки вони надають вам доступ до Інтернету, їхня роль призначити IP-адресу вашому пристрою.
5. Тим не менш ваша IP-адреса може змінитися. Наприклад, увімкнення та вимкнення модему чи маршрутизатора може змінити його. Або ви можете зв'язатися зі своїм Інтернет-провайдером, і вони можуть змінити його для вас.

- б. Коли ви перебуваєте на вулиці, наприклад, подорожуєте, і берете пристрій із собою, домашня IP-адреса не постачається з вами. Це пов'язано з тим, що ви використовуватимете іншу мережу (Wi-Fi у готелі, аеропорту, кав'ярні тощо) для доступу до Інтернету і будете використовувати іншу (і тимчасову) IP-адресу, призначену вам провайдером готель, аеропорт чи кав'ярня. [2]

Існують різні категорії IP-адрес, і в межах кожної категорії різні типи.

- Споживчі IP-адреси

Кожна особа або компанія, що має план обслуговування Інтернету, матиме два типи IP-адрес: їх приватні IP-адреси та їх публічні IP-адреси. Терміни *public* та *private* стосуються розташування мережі - тобто, приватна IP-адреса використовується всередині мережі, тоді як загальнодоступна використовується поза мережею.

- Приватні IP-адреси

Кожен пристрій, який підключається до вашої мережі Інтернет, має приватну IP-адресу. Сюди входять комп'ютери, смартфони та планшети, а також будь-які пристрої з підтримкою Bluetooth, такі як динаміки, принтери або смарт-телевізори. Зі зростанням Інтернету речей кількість приватних IP-адрес у вас вдома, ймовірно, зростає. Маршрутизатору потрібен спосіб ідентифікації цих елементів окремо, а багатьом елементам потрібен спосіб розпізнавання один одного. Таким чином, ваш маршрутизатор генерує приватні IP-адреси, які є унікальними ідентифікаторами для кожного пристрою, який їх диференціює в мережі.

- Загальнодоступні IP-адреси

Загальнодоступна IP-адреса є основною адресою, пов'язаною з усією вашою мережею. Хоча кожен підключений пристрій має власну IP-адресу, вони також входять до основної IP-адреси вашої мережі. Як описано вище, ваша загальнодоступна IP-адреса надається маршрутизатору вашим провайдером. Як правило, провайдери мають великий пул IP-адрес, які вони поширюють серед своїх клієнтів. Ваша загальнодоступна IP-адреса - це адреса,

яку всі пристрої поза вашою Інтернет-мережею використовуватимуть для розпізнавання вашої мережі. [2]

Загальнодоступні IP-адреси бувають двох видів - динамічні та статичні.

Динамічні IP-адреси змінюються автоматично і регулярно. Інтернет-провайдери купують великий пул IP-адрес і автоматично призначають їх своїм клієнтам. Періодично вони перепризначають їх і повертають старіші IP-адреси назад у пул для використання іншими клієнтами. Обґрунтуванням цього підходу є створення економії витрат для Інтернет-провайдера. Автоматизація регулярного переміщення IP-адрес означає, що їм не потрібно виконувати конкретні дії, щоб відновити IP-адресу замовника, якщо вони переїжджають додому, наприклад. Також є переваги безпеки, оскільки зміна IP-адреси ускладнює зловмисникам злом вашого мережевого інтерфейсу. [2]

Статичні IP-адреси на відміну від динамічних IP-адрес залишаються незмінними. Як тільки мережа призначає IP-адресу, вона залишається незмінною. Більшості приватних осіб та підприємств не потрібна статична IP-адреса, але для підприємств, які планують розмістити власний сервер, дуже важливо мати його. Це пов'язано з тим, що статична IP-адреса гарантує, що веб-сайти та адреси електронної пошти, пов'язані з нею, матимуть узгоджену IP-адресу - життєво важливо, якщо ви хочете, щоб інші пристрої могли постійно їх знаходити в Інтернеті.[2]

Мережа IP - це мережа зв'язку, яка використовує протокол Internet Protocol (IP) для надсилання та отримання повідомлень між одним або кількома комп'ютерами. Як одна з найбільш часто використовуваних глобальних мереж, IP-мережа реалізована в мережах Інтернету, локальних мережах (LAN) та корпоративних мережах. IP-мережа вимагає, щоб усі хости або мережеві вузли були налаштовані за допомогою TCP/IP.

Більше того, IP-мережа вимагає, щоб усі підключені пристрої - такі як сервери, комутатори, маршрутизатори та інші пристрої - були налаштовані за допомогою стеку TCP/IP та мали дійсну IP-адресу для здійснення будь-якого мережевого зв'язку. [1]

1.2. IP-телефонія

IP-телефонія (Інтернет-протокол телефонії) - це термін, що використовується для опису технологій, що використовують різноманітні протоколи для обміну голосом, факсом та іншими формами інформації.

IP-телефонія відноситься до будь-якої телефонної системи, яка використовує з'єднання з Інтернетом для надсилання та отримання голосових даних. На відміну від звичайного телефону, який використовує стаціонарні телефони для передачі аналогових сигналів, IP-телефони підключаються до Інтернету через маршрутизатор та модем.

Перший загальнодоступний IP-телефон з'явився на ринку вже в 1995 році. Але, порівняно зі стандартною телефонною системою, він мав низьку якість звуку і був надзвичайно дорогим.

З тих пір технології телефонної мережі, що базуються на Інтернеті, різко покращились. IP-телефонія тепер пропонує якість голосу HD, дешевші експлуатаційні витрати та вдосконалені функції ділового телефону.

Між VoIP та IP телефонією є незначна різниця, хоча терміни часто використовуються як взаємозамінні

IP-телефонія описує будь-яку систему, яка підходить для зони телекомунікацій, що базуються на Інтернеті включаючи факс та інші системи.

Спочатку термін VoIP (Voice over Internet Protocol) був більш конкретним. Це стосувалося лише технології, що використовується для здійснення та отримання телефонних дзвінків через Інтернет.

Однак останніми роками навіть VoIP-провайдери та телекомунікаційні компанії почали використовувати ці терміни як взаємозамінні. І IP-телефонія, і VoIP охоплюють телефонні системи, які використовують LAN (локальну мережу) для підключення до Інтернету через модем/маршрутизатор.[3]

1.3. VoIP

VoIP (передача голосу через Інтернет) - це передача голосу та мультимедійного вмісту через Інтернет. VoIP дозволяє користувачам здійснювати голосові дзвінки з комп'ютера, смартфона, інших мобільних пристроїв, спеціальних телефонів VoIP та браузерів з підтримкою WebRTC. VoIP - це технологія, корисна як для споживачів, так і для бізнесу, оскільки вона, як правило, включає інші функції, яких неможливо знайти у звичайних телефонних послугах. Ці функції можуть включати запис дзвінків, власний ідентифікатор абонента або голосову пошту на електронну пошту. Це також корисно для організацій як спосіб уніфікації комунікацій. [11]

Процес працює аналогічно звичайному телефону, але VoIP використовує підключення до Інтернету замість проводки телефонної компанії. VoIP підтримується групою технологій та методологій, що використовуються для передачі голосового зв'язку через Інтернет, включаючи локальні корпоративні мережі або глобальні мережі. Послуга VoIP перетворює голос користувача з аудіосигналів на цифрові дані, а потім надсилає ці дані через Інтернет. Якщо інший користувач телефонує зі звичайного телефонного номера, сигнал перетворюється назад у телефонний сигнал, перш ніж він надійде до цього користувача.

VoIP також може виконувати маршрутизацію вхідних та вихідних дзвінків через існуючі телефонні мережі. Однак деякі послуги VoIP можуть працювати лише через комп'ютер або телефон VoIP.

VoIP об'єднує комунікаційні технології в одну уніфіковану систему - це означає, що VoIP може використовувати різні аудіо-, відео- або текстові методи зв'язку. Це може бути особливо корисно для бізнесу, тому командам не доводиться працювати з різними додатками, щоб ефективно спілкуватися між собою. [11]

VoIP створює мережу, дозволяючи користувачам телефонувати та проводити веб-конференції за допомогою таких пристроїв, як комп'ютери, смартфони чи інші мобільні пристрої.

Деякі загальні функції можуть включати:

- аудіо дзвінки;
- відео дзвінки;
- голосова пошта;
- миттєві повідомлення;
- командні чати;
- електронна пошта;
- SMS-тексти;
- мобільні та настільні програми;
- дозволяє абоненту вибрати нового телефонного оператора без необхідності нового номера. [11]

1.4. Протоколи VoIP

Основні протоколи VoIP:

- Session Initiation Protocol (SIP)
- H.323
- Media Gateway Control Protocol (MGCP)
- H.248
- Real-time Transport Protocol (RTP)
- Real-time Transport Control Protocol (RTCP)
- Secure Real-time Transport Protocol (SRTP)
- Inter-Asterisk eXchange (IAX)

Розберемо 2 головних детальніше

H.323 - це стандарт МСЕ-Т (Міжнародного союзу телекомунікацій), якого повинні дотримуватися постачальники, надаючи послугу Voice over IP.

Ця рекомендація передбачає технічні вимоги до голосового зв'язку через локальні мережі, припускаючи, що локальні мережі не забезпечують якість обслуговування (QoS). Спочатку він був розроблений для проведення мультимедійних конференцій у локальних мережах, але згодом був розширений, щоб охопити Voice over IP. Перша версія була випущена в 1996 році, тоді як друга версія H.323 набула чинності в січні 1998 року. Стандарт охоплює як точкові, так і багатоточкові конференції. Продукти та програми різних постачальників можуть взаємодіяти, якщо вони дотримуються специфікації H.323. [4]

H.323 визначає чотири логічні компоненти, а саме: термінали, шлюзи, контролери зони та багатоточкові блоки управління (MCU). Термінали, шлюзи та мікроконтролери відомі як кінцеві точки.

Термінали - це кінцеві точки клієнта LAN, які забезпечують двосторонній зв'язок у режимі реального часу. Усі термінали H.323 повинні підтримувати H.245, Q.931, статус прийому реєстрації (RAS) та транспортний протокол реального часу (RTP). H.245 використовується для дозволу використання каналів, Q.931 необхідний для сигналізації виклику та налаштування дзвінка, RTP - транспортний протокол реального часу, який несе голосові пакети, тоді як RAS використовується для взаємодії з контролером зони. Термінали H.323 можуть також включати протоколи конференції даних T.120, відеокодеки та підтримку MCU. Термінал H.323 може взаємодіяти з іншим терміналом H.323, шлюзом H.323 або MCU.

Шлюз H.323 - це кінцева точка мережі, яка забезпечує двосторонній зв'язок у реальному часі між терміналами H.323 в мережі IP та іншими терміналами ITU в комутованій мережі або іншим шлюзом H.323. Вони виконують функцію "перекладача", тобто виконують переклад між різними форматами передачі, наприклад, від H.225 до H.221. Вони також здатні перекладати між аудіо та відео кодеками. Шлюз - це інтерфейс між ТФОП та Інтернетом. Вони беруть голос з комутованої комутаційної мережі та розміщують його у загальнодоступному Інтернеті та навпаки. Шлюзи не є

обов'язковими, оскільки термінали в одній локальній мережі можуть взаємодіяти між собою безпосередньо. Коли терміналам у мережі потрібно взаємодіяти з кінцевою точкою в якійсь іншій мережі, тоді вони здійснюють зв'язок через шлюзи, використовуючи протоколи H.245 та Q.931. [4]

Контролер зони - це найважливіший компонент системи H.323, який відповідає за обов'язки "менеджера". Він виступає центральною точкою для всіх дзвінків у своїй зоні (зона - це агрегація контролера зони та кінцевих точок, зареєстрованих у ній) і надає послуги зареєстрованим кінцевим точкам. Деякі функціональні можливості, які надають контролери зони, перелічені нижче:

- Переклад адреси: Переклад псевдоніма адресований транспортній адресі. Це робиться за допомогою таблиці перекладів, яка оновлюється за допомогою повідомлень про реєстрацію.
- Контроль за допуском: контролери зони можуть надавати або забороняти доступ на основі авторизації викликів, адрес джерела та пункту призначення або деяких інших критеріїв.
- Сигналізація виклику: контролер зони може вибрати завершити сигналізацію виклику з кінцевими точками і може обробити саму сигналізацію виклику. Крім того, контролер зони може направляти кінцеві точки для підключення Канального сигналу безпосередньо один до одного.
- Авторизація викликів: контролер зони може відхиляти дзвінки з терміналу через помилку авторизації за допомогою сигналізації H.225. Причинами відхилення можуть бути обмежений доступ протягом певних періодів часу або обмежений доступ до / з певних терміналів чи шлюзів.
- Управління смугою пропускання: контроль кількості терміналів H.323, яким дозволено одночасний доступ до мережі. Використовуючи сигналізацію H.225, контролер зони може відхиляти дзвінки з терміналу через обмеження пропускну здатності.

- Керування дзвінками: контролер зони може вести список поточних викликів H.323. Ця інформація може бути необхідною, щоб вказати, що викликаний термінал зайнятий, та надати інформацію про функцію управління пропускнуою здатністю.

Багатоточкові блоки управління (MCU) - це кінцева точка мережі, яка забезпечує можливість участі у багатоточковій конференції для трьох або більше терміналів і шлюзів. MCU складається з обов'язкового багатоточкового контролера (MC) та додаткових багатоточкових процесорів (MP). MC визначає загальні можливості терміналів за допомогою H.245, але не виконує мультиплексування аудіо, відео та даних. Мультиплексування медіапотоків обробляється MP під контролем MC. На наступному малюнку показано взаємодію між усіма компонентами H.323. [4]

Протокол ініціації сесії (SIP) - це стандарт IETF для встановлення з'єднань VOIP. Це протокол управління прикладним рівнем для створення, модифікації та завершення сеансів з одним або кількома учасниками. Архітектура SIP схожа на архітектуру HTTP (протокол клієнт-сервер). Запити генеруються клієнтом і надсилаються на сервер. Сервер обробляє запити, а потім надсилає відповідь клієнту. Запит та відповіді на цей запит здійснюють транзакцію. SIP має повідомлення INVITE і ACK, які визначають процес відкриття надійного каналу, через який можуть передаватися повідомлення управління дзвінками. SIP робить мінімальні припущення щодо базового транспортного протоколу. Цей протокол сам забезпечує надійність і не залежить від TCP. SIP залежить від протоколу опису сеансу (SDP) для виконання узгодження для ідентифікації кодека. SIP підтримує описи сеансів, що дозволяють учасникам узгодити набір сумісних типів мультимедіа. Він також підтримує мобільність користувачів за допомогою проксі-сервера та перенаправлення запитів на поточне місцезнаходження користувача. Послуги, які надає SIP, включають [RFC2543]:

- Місцезнаходження користувача: визначення кінцевої системи, яка буде використовуватися для зв'язку

- Налаштування дзвінка: дзвінок та встановлення параметрів дзвінка як для того кому телефонують, так і для того, хто телефонує
- Доступність користувача: визначення готовності зателефонованої сторони брати участь у спілкуванні
- Можливості користувача: визначення носія інформації та параметрів носія, які будуть використовуватися
- Обробка дзвінків: передача та припинення дзвінків

Система SIP складається з двох компонентів:

Агент користувача - це кінцева система, що діє від імені користувача. У ньому є дві частини: клієнт і сервер. Клієнтська частина називається User Agent Client (UAC), а серверна частина - User Agent Server (UAS). UAC використовується для ініціювання запиту SIP, тоді як UAS використовується для отримання запитів та повернення відповідей від імені користувача.

Мережеві сервери - У мережі є 3 типи серверів. Сервер реєстрації отримує оновлення щодо поточного місцезнаходження користувачів. Проксі-сервер при отриманні запитів пересилає їх на сервер наступного переходу, який має більше інформації про місцезнаходження викликаної сторони. Сервер переадресації при отриманні запитів визначає сервер наступного переходу та повертає клієнту адресу сервера наступного переходу замість пересилання запиту.

SIP визначає багато повідомлень. Ці повідомлення використовуються для зв'язку між клієнтом та SIP-сервером. Ці повідомлення:

- INVITE: для запрошення користувача до дзвінка
- BYE: для розриву зв'язку між двома кінцевими точками
- ACK: для надійного обміну повідомленнями-запрошеннями
- OPTIONS: для отримання інформації про можливості дзвінка
- REGISTER: надає інформацію про місцезнаходження користувача на сервері реєстрації SIP.
- CANCEL: для припинення пошуку користувача. [4]

Виклики та абоненти ідентифікуються за SIP-адресами. Під час здійснення SIP-дзвінка абоненту спочатку потрібно знайти відповідний сервер і надіслати йому запит. Абонент може або безпосередньо зв'язатися з абонентом, або побічно через сервери перенаправлення. Поле ідентифікатора виклику в заголовку повідомлення SIP однозначно ідентифікує дзвінки.

Як протокол виконує операції:

SIP-адресація - хости SIP ідентифікуються за URL-адресою SIP, яка має форму sip:username@host. SIP-адреса може позначати як особу, так і цілу групу.

Розташування SIP-сервера - клієнт може або надіслати запит на проксі-сервер SIP, або може надіслати його безпосередньо на IP-адресу та порт, що відповідають єдиному ідентифікатору запиту (URI).

SIP-транзакція - після того, як основна частина URI запиту буде вирішена на SIP-сервері, клієнт може надсилати запити на цей сервер. Запит разом із відповідями, викликаними цим запитом, складає транзакцію SIP. Запити можуть бути надіслані через надійний TCP або через ненадійний UDP.

Запрошення SIP - успішне запрошення SIP складається з двох запитів: INVITE, а потім ACK. Запит INVITE просить абонента приєднатися до певної конференції або встановити двосторонню розмову. Після того, як абонент погодився взяти участь у дзвінку, абонент підтверджує, що отримав відповідь, надіславши запит ACK. Запит INVITE містить опис сеансу, який надає викликаній стороні достатньо інформації для приєднання до сесії. Якщо абонент хоче прийняти дзвінок, він відповідає на запрошення, повертаючи аналогічний опис сеансу.

Пошук користувача - визваний може з часом змінювати своє положення. Ці місця можна динамічно реєструвати на SIP-сервері. Коли SIP-сервер запитує про місцезнаходження абонента, він повертає список можливих розташувань. Сервер розташування в системі SIP фактично генерує список і передає його серверу SIP. [4]

Зміна існуючої сесії - іноді нам може знадобитися змінити параметри існуючого сеансу. Це робиться шляхом повторної публікації повідомлення INVITE з використанням того самого ідентифікатора виклику, але нового тіла для передачі нової інформації. [4]

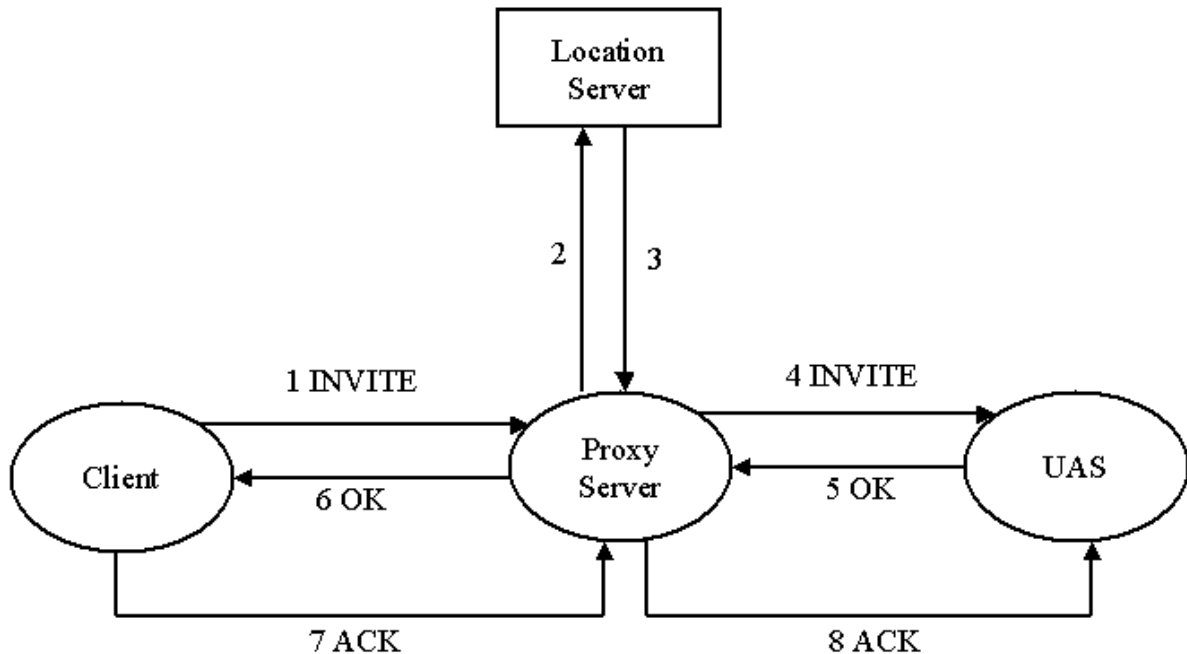


Рис.1.1 Приклад операції SIP

Порівняння H.323 з SIP:

- Оскільки H.323 був розроблений з урахуванням сигналів ATM та ISDN, тому H.323 не дуже підходить для управління голосом через IP-системи.
- H.323 за своєю суттю є складним, має накладні витрати і, отже, неефективний для VOIP.
- H.323 не має розширюваності, необхідної для протоколу сигналізації для VOIP. Оскільки SIP розроблявся з урахуванням Інтернету, він дозволяє уникнути підводних каменів як складності, так і розширюваності. SIP повторно використовує більшість полів заголовка, правила кодування, коди помилок та механізми

автентифікації HTTP. H.323 визначає сотні елементів, тоді як SIP має лише 37 заголовків, кожен з невеликою кількістю значень і параметрів.

- H.323 використовує двійкове представлення для своїх повідомлень, яке базується на ASN.1, тоді як SIP кодує свої повідомлення як текст, подібно до HTTP.
- H.323 не дуже масштабований, оскільки він був розроблений для використання в одній локальній мережі і тому має деякі проблеми при масштабуванні, хоча новіші версії пропонують способи вирішення проблеми.
- H.323 все ще обмежений при виконанні виявлення циклу в складних багатодомених пошуках. Це можна зробити з великим збереженням повідомлень, але цей прийом не дуже масштабований. З іншого боку, SIP використовує метод виявлення циклу, перевіряючи історію повідомлення в полях заголовка, що може бути зроблено способом без стану.

Перевага SIP полягає в тому, що він підтримується IETF, одним з найважливіших стандартних органів, тоді як перевага H.323 полягає в тому, що в даний час він має набагато більший обсяг ринку. [4]

ВИСНОВКИ ДО РОЗДІЛУ 1

У даному розділі було проаналізовано роботу IP-мереж, а також переваги та можливості VoIP телефонії.

Також були проаналізовані основні протоколи VoIP, детально розглянуті протоколи SIP та H.323, їх переваги та недоліки, принципи роботи та актуальність використання цих протоколів на сьогоднішній день.

РОЗДІЛ 2

VOIP ОБЛАДНАННЯ, ASTERISK ТА SI2000

2.1. VoIP обладнання

Основним обладнанням що використовуються для VoIP є:

IP АТС - це багатофункціональна телефонна система, яка комутує голосові і відео виклики по IP мережі. Голос і відео передаються як потік даних (IP пакети) . Тобто IP АТС це метафоричний центр вашої телефонної системи.

IP АТС бувають таких типів:

- Апаратні IP-АТС - поставляється у вигляді спеціалізованого обладнання з встановленим ПЗ. У подібних рішеннях апаратна частина не підлягає удосконаленню CPU, DDR, HDD, PRI і масштабування проводиться не так ефективно. Основні представники: AddPac, Alcatel, Avaya, Cisco, ISKRATEL, Nortel, Panasonic, Zultys.
- Програмні IP-АТС - поширюється у вигляді готових Linux-дистрибутивів або виконуваних файлів під операційну систему Windows: 3CX, AsteriskNow, FreePBX, Elastix, PTU, Zeon, WELLtime. Переваги даного класу - можливість роботи в віртуальному оточенні Vmware, XEN, KVM, VirtualBox і можливість гнучко вибирати апаратні характеристики. За допомогою спеціалізованих PCI-плат Digium, OpenVox, Sangoma можна підключити IP-АТС до вже наявної інфраструктури по цифровим портам PRI, ISDN BRI і аналоговим FXO, FXS.
- Віртуальні АТС - послуга операторів телефонного зв'язку або Інтернет-провайдерів з організації корпоративної телефонії за рахунок застосування Інтернету та обладнання IP-телефонії (зокрема VoIP-телефонів) в офісі компанії-клієнта і виділеної

програмної АТС або віртуальної сутності (наприклад домену або чогось подібного) на софтвері або апаратної АТС телекомунікаційної компанії.[6]

Шлюз VoIP - ці шлюзи виступають мостом між традиційною телефонною інфраструктурою та комп'ютерною мережею. Цей пристрій перетворює аналогові телефонні сигнали в SIP (Session Initiation Protocol) і навпаки. Більш надійні шлюзи можуть одночасно приймати до 256 дзвінків.

Існує три типи шлюзів:

- Аналог з портами FXO / FXS - від 2 до 24 ліній. Шлюз FXS підключає аналогові телефони безпосередньо до АТС. Шлюз FXO з'єднує міську телефонну лінію з АТС.
- Цифровий - підключення європейських або американських цифрових ліній BRI ISDN, PRI / E1, T1 (одна або кілька ліній). Вони підходять для підключення до АТС або в розриві між приватною АТС з обсягом 50 абонентів та міською телефонною мережею без реконфігурації. Робота через протоколи ISDN, SS7 та QSIG.
- Шлюзи GSM SIP - Вони мають спеціальні слоти для SIM-карт для підключення стільникових телефонів до мережі IP та АТС. [7]

IP-маршрутизатор - маршрутизатор спрямовує інтернет-трафік, передаючи пакети даних між комп'ютерними мережами. Це те, що підключає ваші пристрої з підтримкою VoIP до Інтернету і відповідає за якість вашого дзвінка та зв'язок



Рис. 2.1 Маршрутизатор MikroTik RB4011iGS+RM

Аналоговий телефонний адаптер - цей пристрій, також відомий як АТА, дозволяє використовувати стандартний телефон для дзвінків через IP-мережу.



Рис. 2.2 АТА Grandstream HT802

IP-телефон - IP-телефон, також відомий як VoIP-телефон, - це фізична телефонна система, яка використовує технологію VoIP замість традиційної телефонної лінії. Телефон підключається до Інтернету за допомогою кабелю Ethernet, що має велику пропускну здатність Інтернету, який потім підключається до IP-адреси вашого VoIP-провайдера. [5]

Два основних типи телефонів VoIP - апаратні та програмні. Апаратний VoIP-телефон виглядає як традиційний дротовий або бездротовий телефон і включає подібні функції, такі як динамік або мікрофон, тачпад та дисплей ідентифікатора абонента. VoIP-телефони також можуть забезпечувати голосову пошту, конференц-зв'язок та переадресацію дзвінків.



Рис. 2.3 IP-телефон

Програмні IP-телефони, також відомі як софтфони, - це програмні клієнти, встановлені на комп'ютері чи мобільному пристрої. Інтерфейс користувальницького телефону часто виглядає як телефонна слухавка з тачпадом та дисплеєм ідентифікатора абонента. Гарнітура підключається до комп'ютера або мобільного пристрою для здійснення дзвінків. Користувачі також можуть телефонувати через свій комп'ютер або мобільний пристрій, якщо у них є вбудований мікрофон та динамік. [11]

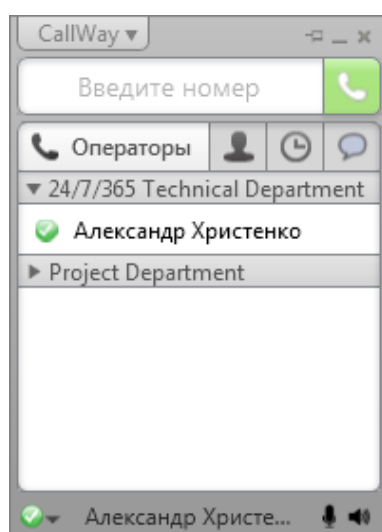


Рис. 2.4 Софтфон

VoIP-гарнітура - це навушники з вбудованим мікрофоном. Це не є життєво важливим обладнанням для вашої телефонної системи, але вона дозволить вам використовувати софтфон.

2.2. Основні кодеки які використовуються в VoIP

- G.711 - це самий базовий кодек ТМЗК (PSTN). В рамках даного кодека використовується імпульсно-кодова модуляція PCM. Всього в світі використовується 2 методу посилення сигналу G.711: μ - закон в Північній Америці і A - закон в іншій частині світу. Даний кодек передає 8 - бітове слово 8 000 разів в секунду.

Якщо помножити 8 на 8 000, отримаємо: 64 000 біт - тобто 64 Кб/с, швидкість потоку, створюваного G.711.

Важлива особливість G.711 в тому, що він мінімально завантажує процесор машини, на якій він запущений.

- G.726 - використовувався деякий час, ставши заміною для G.721, який на той момент застарів, і є одним з перших кодеків з алгоритмом компресії. Він так само відомий як кодек з адаптивною імпульсно-ковою модуляції (Adaptive Differential Pulse-Code Modulation, ADPCM) і може використовувати кілька швидкостей потоку передачі. Найбільш поширені швидкості передачі це 16, 24 і 32 Кб/сек.

Кодек G.726 майже ідентичний G.711 - єдиною відмінністю є те, що він використовує половину смуги пропускання. Це досягається шляхом того, що замість відправки повного результату квантування, він відправляє тільки різницю між двома останніми вимірюваннями. У 1990 році від кодека практично відмовилися, так як він не міг працювати з факсимільними сигналами і модемами. Але в наш час, з - за своєї економії смуги пропускання і ресурсів центрального процесора у нього є всі шанси знову стати популярним кодеком в сучасних мережах. [8]

- G.729A - з огляду на те, яку малу смугу пропускання використовує G.729A, всього 8 Кб/сек., Він забезпечує чудову якість зв'язку. Це досягається за рахунок використання поєднаної структури з керованим алгебраїчним кодом і лінійним передбаченням (Conjugate-Structure Algebraic-Code-Excited Linear Prediction, CS-ACELP). Унаслідок патенту, використання даного кодека є комерційним; проте це не заважає кодеку G.729A бути популярним в різних корпоративних мережах і телефонних системах.

Для досягнення такого високого ступеня стиснення, G.729A активно задіює потужності процесора (CPU). [8]

- GSM - кодек для глобального стандарту цифрового мобільного стільникового зв'язку (Global System for Mobile Communications, GSM) не обтяжений ліцензуванням, як його аналог G.729A, але пропонує високу якість і помірну навантаження на процесор при використанні 13 Кб/сек. смуги пропускання. Експерти вважають, що якість GSM трохи нижче ніж G.729A.
- iLBC - кодек iLBC (Internet Low Bitrate Codec) поєднує в собі низьке використання смуги пропускання і високої якості. Даний кодек ідеально підходить для підтримки високої якості зв'язку в мережах з втратами пакетів.

iLBC не такий популярний як кодеки стандартів ITU і тому, може бути несумісний з популярними IP - телефонами і IP - АТС. Інженерний рада Інтернету (IETF) випустив RFC 3951 і 3952 на підтримку кодека iLBC.

Internet Low Bitrate кодек використовує складні алгоритми для досягнення високого показника стиснення, тому, досить відчутно завантажує процесор.

Кодек iLBC працює на швидкості в 13.3 Кб / сек. з фреймами в 30 мс, і на швидкості 15.2 кб / сек. з фреймами в 20 мс. [8]

- Speex - кодек Speex відноситься до сімейства кодеків змінної швидкості (variable-bitrate, VBR), що означає можливість кодека динамічно змінювати швидкість передачі бітів в залежності від статусу продуктивності мережі передачі. Цей кодек пропонується в широкосмугових і вузькосмугових модифікаціях, в залежності від вимоги до якості.

Speex повністю безкоштовний і поширюється під програмної ліцензією університету Берклі (Berkeley Software Distribution

license, BSD). Кодек працює на діапазонах від 2.15 до 22.4 Кб / сек. в рамках змінного бітрейта.

- G.722 - є стандартом ITU-T (International Telecommunication Union - Telecommunication sector) і вперше опублікований в 1988 році. Кодек G.722 дозволяє забезпечити якість, не нижче G.711 що робить його привабливим для сучасних VoIP розробників. На даний момент патент на G.722 не дійсний, і цей кодек є повністю безкоштовним. [8]

Таблиця 1.1

Порівняння деяких кодеків які використовуються в VoIP

Кодек	Якість Аудіо	Навантаження CPU	Розмір пакету	Загальний розмір (базовий + заголовки)
G711	Хороше	Дуже мале	64 кб/с	95.2 кб/с
G722	Дуже хороше	Мале	64 кб/с	95.2 кб/с
GSM	Прийнятне	Середнє	13 кб/с	44.2 кб/с
G729	Середнє	Високе	8 кб/с	39.2 кб/с

Деякі зауваження щодо використання кодеків:

- Дані представлені для одного аудіо потоку. VoIP виклики використовують один потік для кожного з напрямків. Тому розмова між 2 абонентами вимагає подвійну смугу пропускання
- G729 забезпечує невелику смугу пропускання і загалом хорошої якості. Однак, потрібно враховувати 2 недоліки:
- Ефективність має ціну у вигляді завантаження CPU. Чим інтенсивніше використовується процесор тим більше можна стиснути голос при збереженні якості мови.

- G729 "закритий" кодек. Тому кількість викликів з G729 не перевищує половини ліній 3CX Phone System simultaneous call license.
- Тому, G729 потрібно використовувати тільки у випадках коли він реально потрібен, для зовнішніх викликів через VoIP Providers, дзвінки через Тунелі, або для віддалених абонентів (як правило всі виклики через Інтернет).
- Хоча G711 і G722 використовують вдвічі більшу смугу ніж будь-який інший кодек, більшість локальних мереж здатні витримати таке навантаження. [9]

Процес надсилання даних іншим користувачам включає інкапсуляцію звуку в пакети даних, передачу пакетів через IP-мережу та деінкапсуляцію пакетів назад в аудіо на іншому кінці з'єднання.

У корпоративних або приватних мережах якість обслуговування (QoS), як правило, використовується для визначення пріоритету голосового трафіку перед програмами, що не сприймають затримки, для забезпечення прийнятної якості голосу.

Система VoIP також може включати бази даних відстеження місцеположення для платформ маршрутизації та управління викликами E911 (покращений 911). Це може збирати статистику ефективності дзвінків для реактивного та активного управління якістю голосу.

Усуваючи мережі з комутацією каналів для голосових комунікацій, VoIP зменшує витрати на мережеву інфраструктуру та дозволяє постачальникам надавати голосові послуги через широкосмугові та приватні мережі. Це також має дозволити підприємствам управляти єдиною мережею передачі голосу та даних.

VoIP також сприяє стійкості мереж на основі IP, забезпечуючи швидкий збій після відключень та надмірного зв'язку між кінцевими точками та мережами. [11]

2.3. Asterisk

Asterisk (PBX) (Private Branch Exchange) — відкрита комунікаційна платформа, котра використовується для розгортання програмних АТС, систем голосового зв'язку, VoIP-шлюзів, організації IVR-систем (голосове меню), голосової пошти, телефонних конференцій і call-центрів.

Asterisk може взаємодіяти за стандартами Voice-over-IP [VoIP] (SIP, H.323, IAX та інші), а також з громадськими комутованими телефонними мережами (Public Switched Telephone Network — PSTN) за допомогою підтримуваного апаратного забезпечення.

Відкритий вихідний код від компанії Digium, початково створений Марком Спенсером. Програмний комплекс працює у середовищі Linux, FreeBSD, OpenBSD і Solaris тощо. Назва проекту походить від назви символу «*» (англ. asterisk — «зірочка»).

Для розширення функцій можна написати план нумерації власною мовою Asterisk, написати модуль на мові Сі, чи скористатись AGI — гнучким універсальним інтерфейсом для інтеграції з зовнішніми системами обробки даних. Модулі, які виконуються через AGI, можуть бути написані будь-якою мовою програмування.

Asterisk розповсюджується на умовах подвійної ліцензії, завдяки якій одночасно з основним кодом, котрий розповсюджують за відкритою ліцензією GNU GPL, можливе створення закритих модулів, які містять ліцензований код, як от: модуль для підтримки кодека G.729. [12]

Asterisk - це основа для створення мультипротокольних програм і рішень для спілкування в режимі реального часу. Asterisk стосується голосових та відеопрограм в режимі реального часу, як Apache до веб-програм: основна платформа. Asterisk абстрагується від складності комунікаційних протоколів та технологій, що дозволяє зосередитися на створенні інноваційних продуктів та рішень.

Ви можете використовувати Asterisk для створення комунікаційних програм, таких як телефонні системи для бізнесу (також відомі як IP-АТС), розподільники дзвінків, VoIP-шлюзи та конференц-мости. Asterisk включає компоненти як низького, так і високого рівня, що значно спрощує процес побудови цих складних додатків. [13]

2.4. ISKRATEL SI2000

SI-2000 - це сучасна цифрова комутаційна система з керуванням по записаній програмі, призначена для використання на ТМЗК. Цифрові станції SI-2000 можуть використовуватися в якості місцевих або транзитних АТС на мережах зв'язку загального користування або відомчих мережах



Рис. 2.5 ISKRATEL SI2000 зовні



Рис. 2.6 ISKRATEL SI2000 всередині

Інтегрований програмний комутатор (iCS - integrated call server) є ідеальним рішенням для телекомунікаційних операторів, які не бажають модернізувати існуючої мережі, але в той же час ще не підготовлених до комплексного IP-рішення.

Час телефонних станцій на основі технологій комутації каналів добігає кінця.

Оператори шукають рішення, що базуються на технологіях VoIP. Конвергентні мережі з серверами обробки викликів і з розподіленою архітектурою поступово стають реальністю, хоча є безліч випадків, де повний перехід є передчасним. Саме тому інтегрований програмний комутатор є ідеальним рішенням, так як він просто впроваджується в існуючі TDM мережі і дозволяє будувати мережу, що базується на технологіях VoIP. Істотною перевагою інтегрованого програмного комутатора є можливість простого переходу в розподілену мережу з програмним комутатором, як наступний крок в розвитку NGN. [14]

Інтегрований програмний комутатор SI2000 є передовою відкритою платформою для побудови телекомунікаційних мереж і мереж передачі даних.

Призначений для використання на всіх ринках, а саме:

- в мережі загального користування як:
- кінцева станція з можливістю підключення аналогових, ISDN і IP користувачів,
- концентратор,
- перетворювач сигналізацій,
- вузол послуг,
- медіа-шлюз (MGW);
- як самостійна система УПАТС,
- у відомчій мережі на всіх рівнях мереж

Система містить набір інтерфейсів і сигналізацій.

Включення в PSTN і відомчу мережу за допомогою:

- цифрових сигналізацій CAS,
- аналогових сигналізацій (E & M), [14]

Включення в відомчу ISDN мережу або в ISDN мережу загального користування за допомогою сигналізацій CCS:

- SSN7,
- DSS1
- QSIG

Реалізація функціональності VoIP trunking:

- SIP-T
- H.323

Підключення різного абонентського обладнання:

- аналогові термінали,
- IP-термінали (SIP і H.323)
- термінали ISDN (по Uk0- і S0-інтерфейсів),
- термінальне обладнання ISDN PRA за допомогою інтерфейсу S2M,
- аналогові і цифрові HE-ISDN термінали (ПК, модеми, та ін., Які не є ISDN терміналами) за допомогою термінальних адаптерів,

- аналоговий абонентський концентратор AXM (ASM модулі SI2000 V4) або ANA - вузол доступу типу А, що підтримує підключення тільки аналогових абонентів,

- ISDN УПАТС системи (за допомогою інтерфейсу BRA / Uk0, або за допомогою інтерфейсу PRA / S2M),

- Базові станції системи Philips для підключення радіо ліній DECT-DAS, за допомогою інтерфейсу для підключення базових станцій Philips (4-провідні та 2 Мбіт / с). DECT-DAS інтегрований з LS5092AX і з'єднаний з MLC по інтерфейсу PRA / S2M,

- Базові станції системи DeTeWe для підключення радіо ліній IP-DECT, як багатовхідні IP-термінали по протоколу H.323,

- УПАТС на аналоговій абонентській лінії за допомогою інтерфейсу Z1,

- аналогові і цифрові HE-ISDN УПАТС системи (за допомогою аналогових і цифрових сигналізацій CAS),

- інтерфейси для дротових мереж передачі даних (X.21, X.21 bis, X.20 bis), що підключаються за допомогою відповідних термінальних адаптерів по DSS1; [14]

- Підключення вузлів доступу за допомогою:

- інтерфейсу V5.1 і

- інтерфейсу V5.2. Умовні позначення: [14]

Умовні позначення:

TPE - інтерфейс первинного доступу PRA (Primary Rate Access), Ver. E

CDG - комунікаційний контролер, версія G

IDE - інтерфейс для вбудовування пам'яті FLASH або жорсткого диска

MUX - комутаційне поле з паралельно-послідовним перетворювачем даних PCM

LSL - послідовні з'єднання 16 Мбіт / с між інтерфейсами LSL (Low Speed Link) периферійних плат і платою CLC - контролер лінійного модуля, версія C

SAX - плата портів аналогових абонентських ліній, версія x

- SBx - плата основного доступу BRA (Basic Rate Access), версія x
- TAx - плата портів аналогових сполучних ліній
- DC / DC - схема генерування вторинних значень напруги живлення
- KLB - плата випробування абонентських ліній і аналогових телефонних апаратів, версія B
- PLC - плата електроживлення, версія C
- UB - напруга батарейного живлення [14]

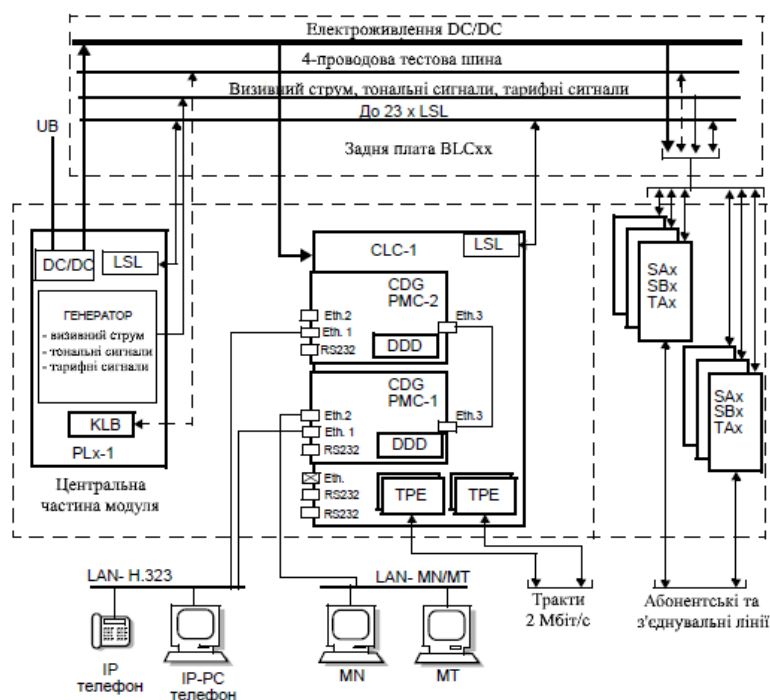


Рис.2.7 Блок-схема модуля MLC ATC SI-2000

ВИСНОВКИ ДО РОЗДІЛУ 2

У даному розділі було розглянуто основне обладнання що використовується в VoIP таке як IP АТС, шлюз VoIP, IP-маршрутизатор, АТА, IP-телефон та VoIP-гарнітура.

Були проаналізовані та порівняні між собою кодеки які використовуються в VoIP.

Також було розглянуто основні переваги IP-АТС Asterisk та цифрової АТС ISKRATEL SI2000.

РОЗДІЛ 3

ПОБУДОВА КАНАЛУ ЗВ'ЯЗКУ МІЖ ASTERISK ТА SI2000

3.1. Конфігурування iCS з функціями IP-шлюзу

IP-шлюз - спосіб використання вузла iCS, коли він працює як медіа шлюз і шлюз сигналізації між мережами TDM і IP. Розмовний телефонний трафік перетворюється в RTP, а TDM сигналізації (SS7, DSS1) в IP-сигналізації (SIP-T, H.323). В рамках конфігурації IP-шлюзу ви будете встановлювати комунікацію з іншими вузлами - з IP-шлюзом з IP-мережі, а також з іншим вузлом (телефонною станцією) в мережі TDM.[15]

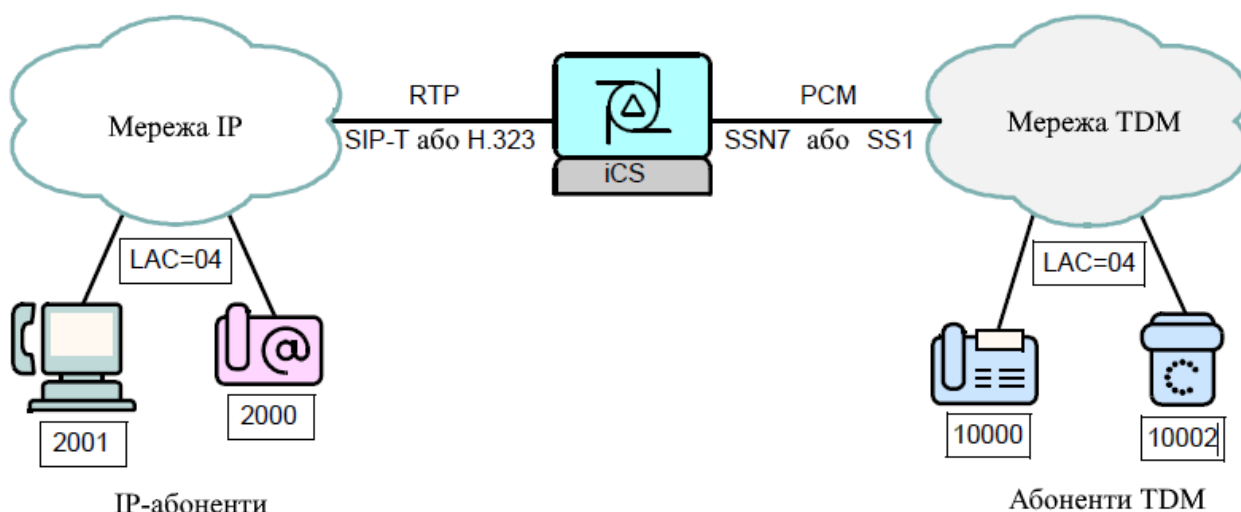


Рис. 3.1 Приклад IP-шлюзу з з'єднанням в мережі TDM і IP

Першим кроком в підключенні IP-шлюзу до IP-мережі є налаштування інтерфейсу Ethernet, який ви будете використовувати для зв'язку, і привласнення IP-адреси інтерфейсу.

1) Налаштування мережевого IP-з'єднання включає наступні процедури, що виконуються в наступному порядку:

1.1. «Управління інтерфейсом Ethernet для зв'язку з IP-мережею».

1.2. «Управління IP-адресами для підключення до IP-мережі».

Відкриваємо систему управління, обираємо вузол та натискаємо CMG

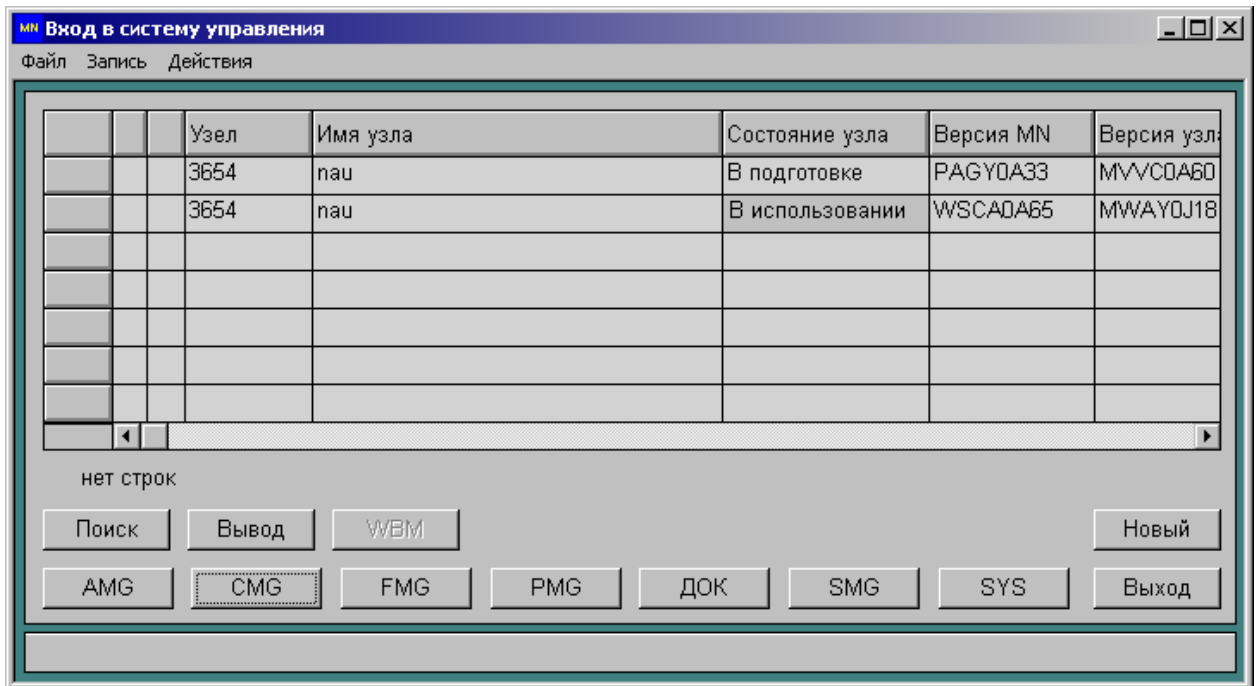


Рис. 3.2 Вхід до системи управління

Обираємо команду Mode & Seizure > Set Mode & Select Node

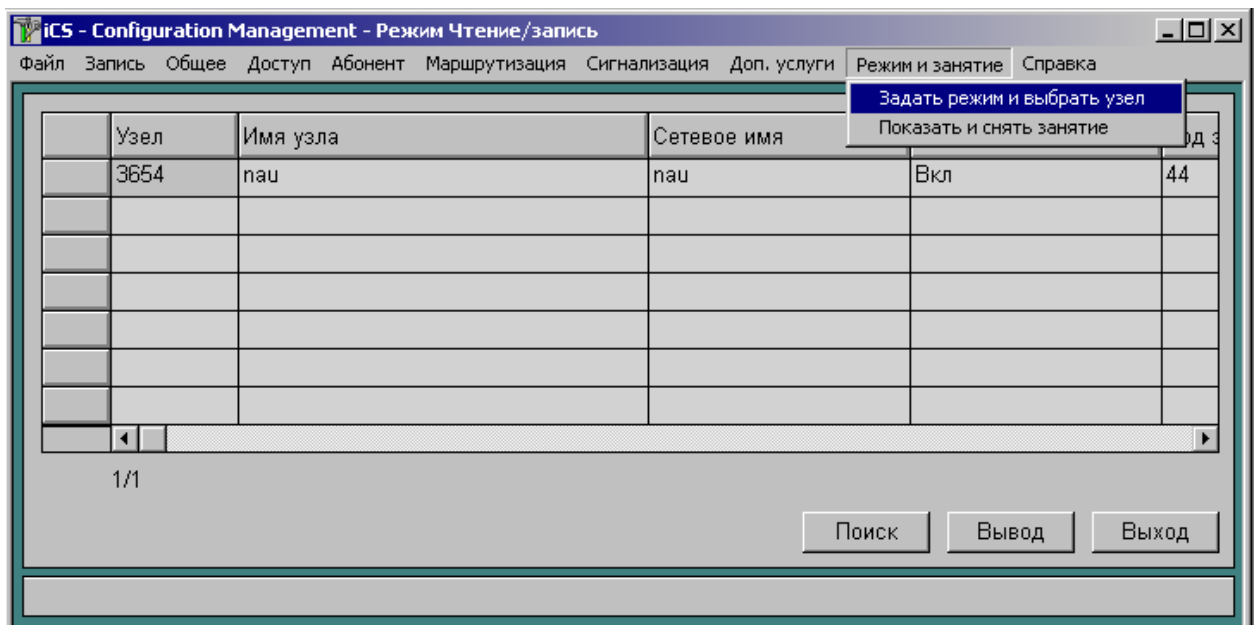


Рис. 3.3 Меню CMG

В рамці Application Mode відмічаємо поле режиму Read/Write і
установлюємо курсор в поле Status

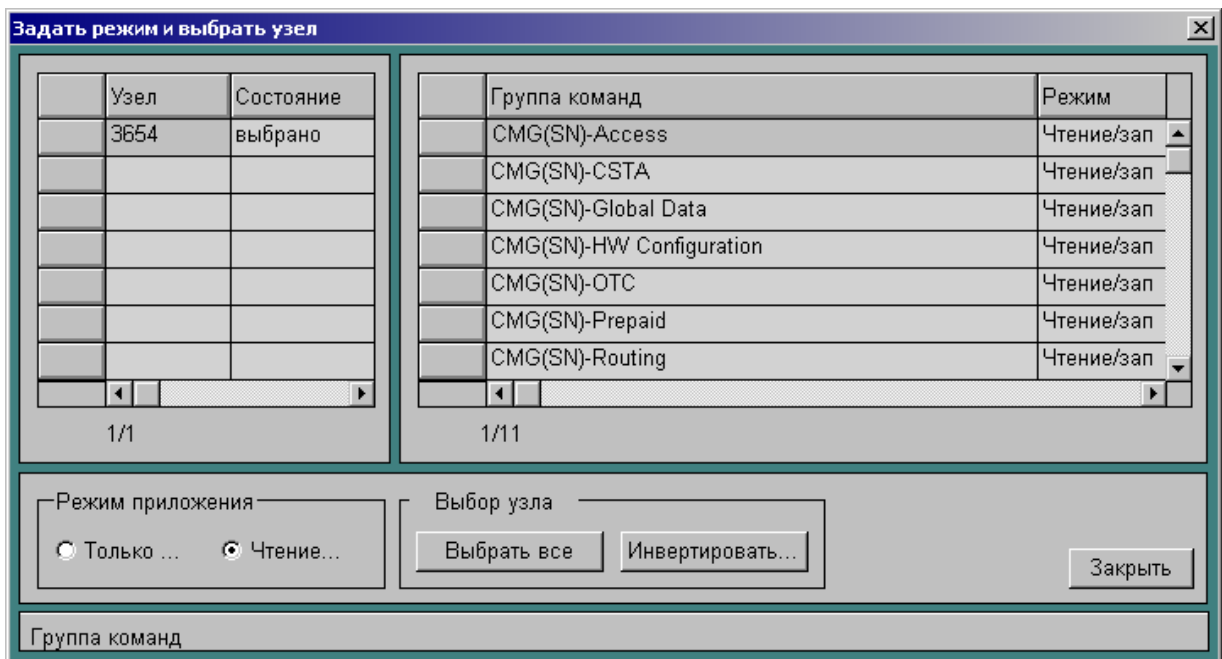


Рис. 3.4 Вибір режиму та вузла для введення змін

1.1. Для налаштування інтерфейса Ethernet для зв'язку з IP-мережею
обираємо команду CMG > Signalling > Ethernet Interface

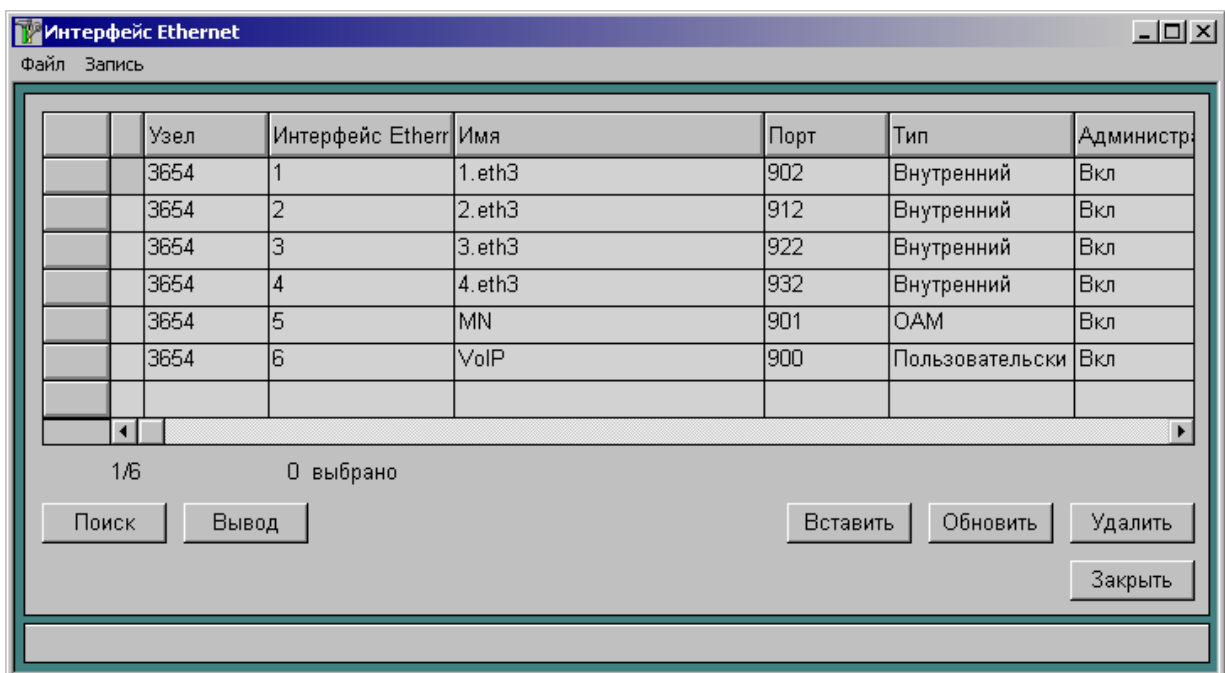


Рис. 3.5 Налаштування інтерфейсів Ethernet

Натискаємо Insert задаємо параметри Ethernet Interface, Ethernet Name, Port, Ethernet Type.

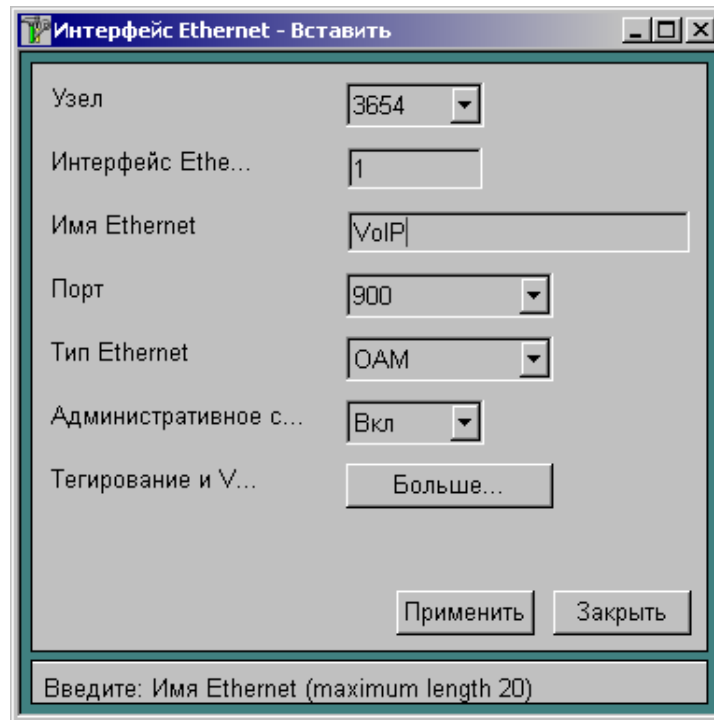


Рис. 3.6 Додаємо інтерфейс Ethernet

1.2. Для управління IP-адресами для підключення до IP-мережі обираємо команду SYS > Administration > IP Network > IP Address.

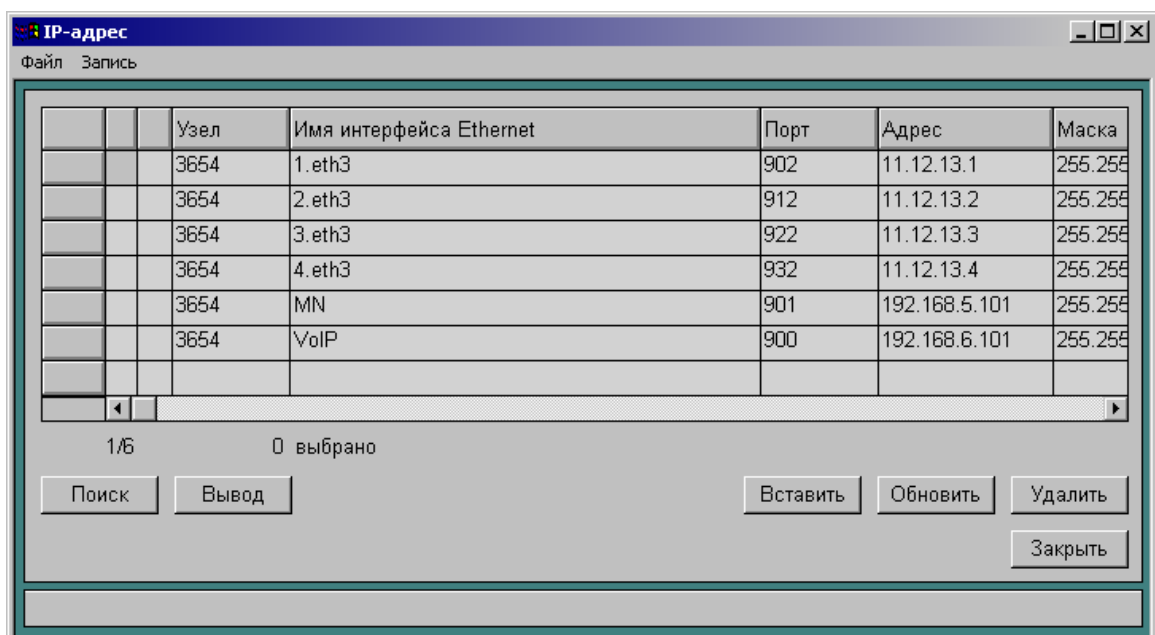


Рис. 3.7 Налаштування IP-адреси для з'єднання з мережею IP

Натискаємо Insert задаємо параметри Ethernet Interface Name, Address, Mask, Metric, Function.

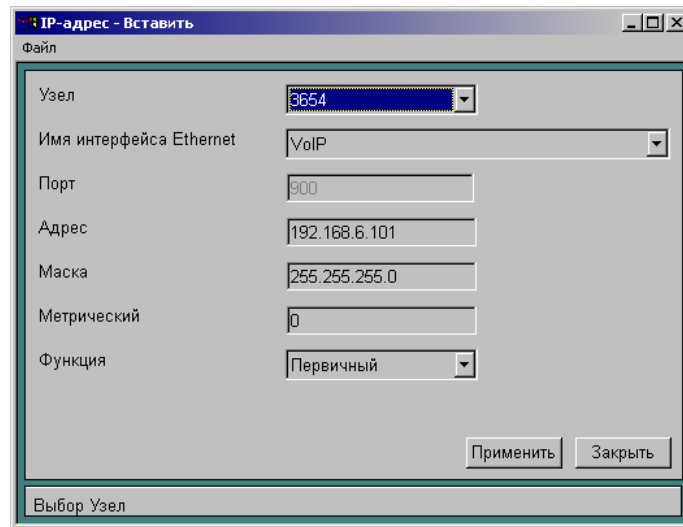


Рис. 3.8 Додаємо адресу серверу з Asterisk

2) Управління сполучними лініями IP виконуються в такому порядку:

2.1. "Адміністрування модуля IP".

2.2. "Адміністрування групи з'єднувальних ліній IP".

2.3. "Внесення сполучних ліній IP".

2.1. Для налаштування модуля IP обираємо команду CMG > Global > HW Configuration > Module

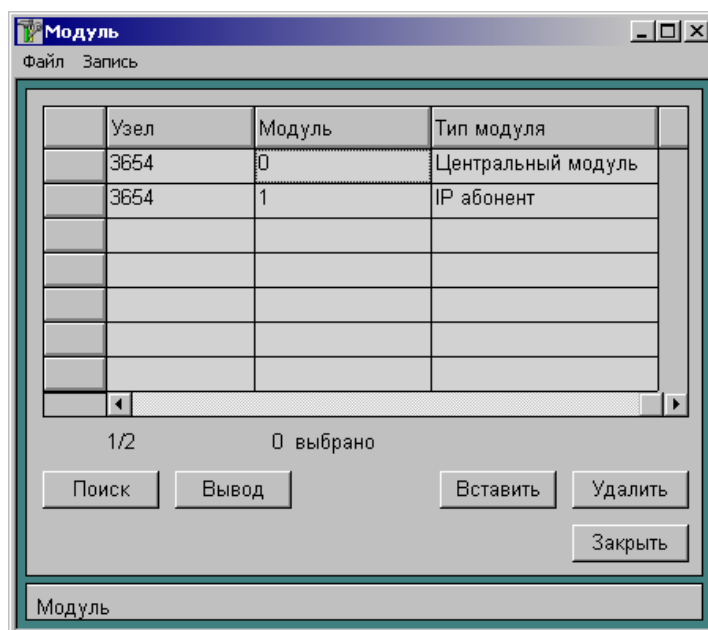


Рис. 3.9 Вікно Module

Натискаємо Insert, вписуємо номер модуля, в поле Module Type вибираємо значення IP

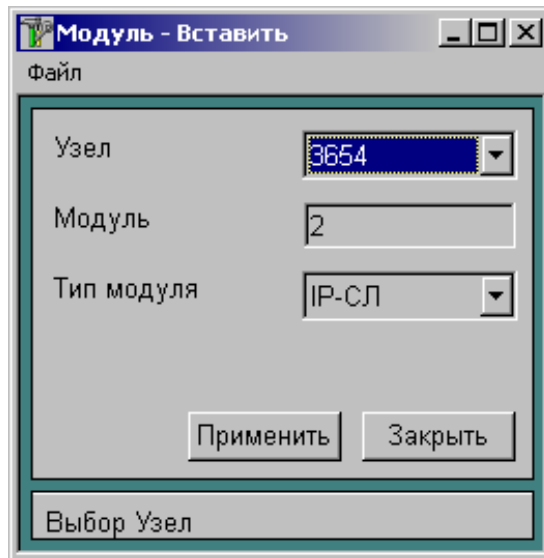


Рис. 3.10 Додаємо модуль

2.2 Для налаштування групи з'єднувальних ліній IP обираємо команду CMG > Routing > Trunk Group > Global

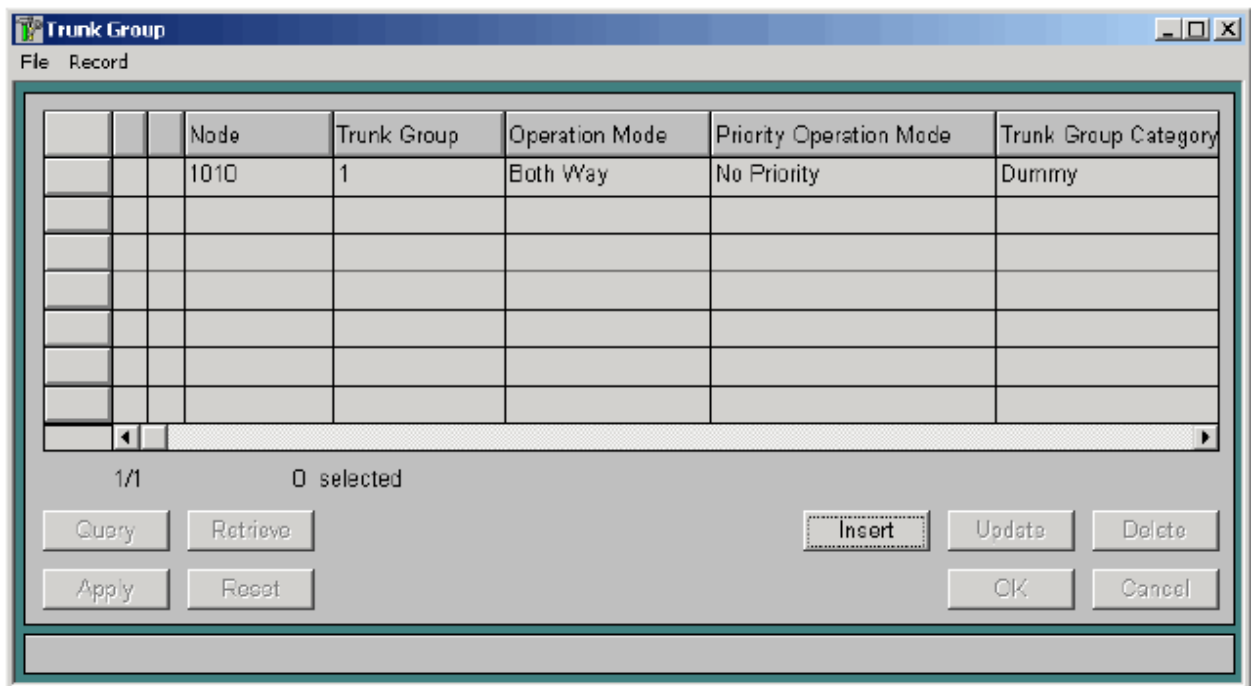


Рис. 3.11 Список груп з'єднувальних ліній

Натискаємо Insert задаємо параметри Trunk Group, Register Signalling Type, DSS1 / QSIG & ISUP & CAS Register Variant, Trunk Offering Type

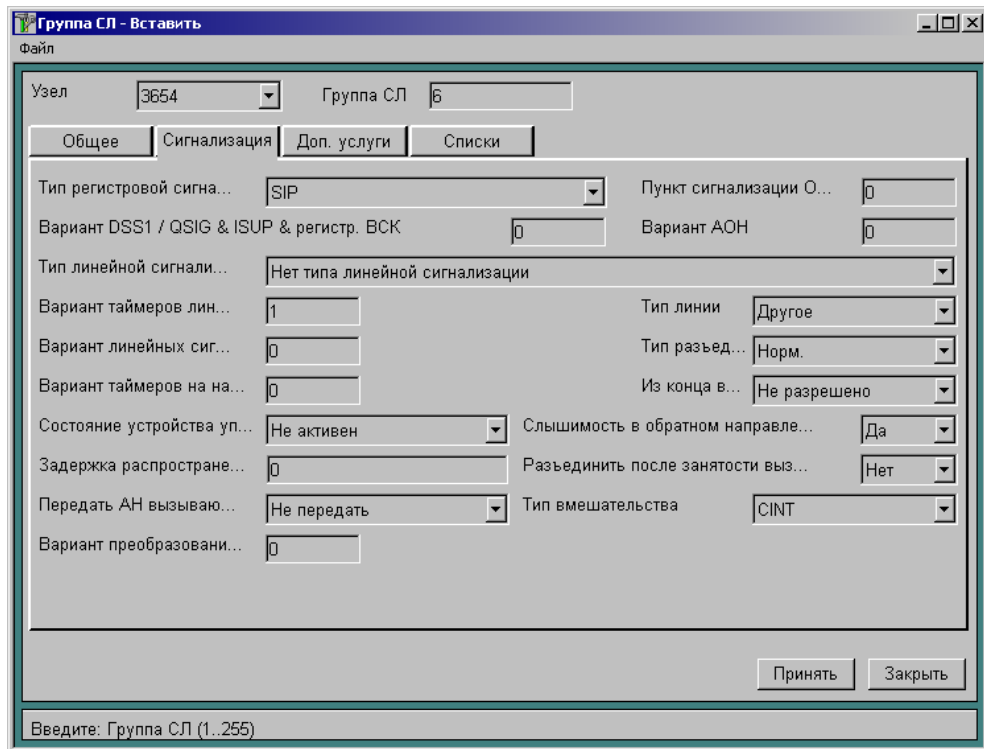


Рис. 3.12 Параметры группы з'єднувальних ліній

2.3. Для внесення сполучних ліній IP обираємо команду CMG > Routing > Trunk > IP.

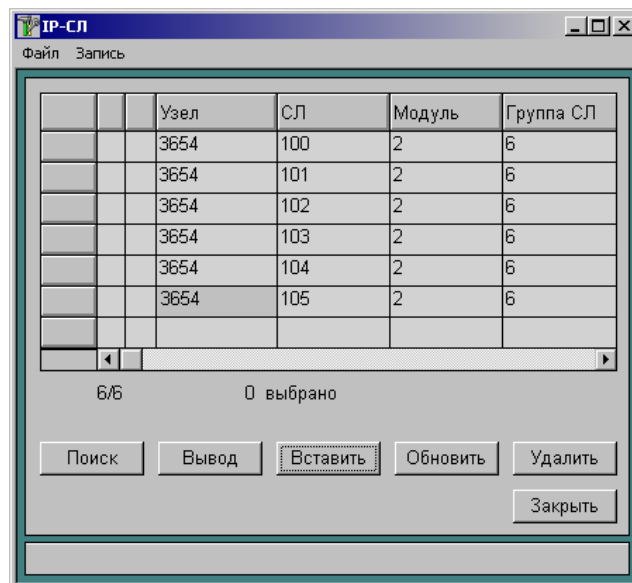


Рис. 3.13 З'єднувальні лінії

Натискаємо Insert задаємо параметри Module, Start Trunk, End Trunk, Trunk Group

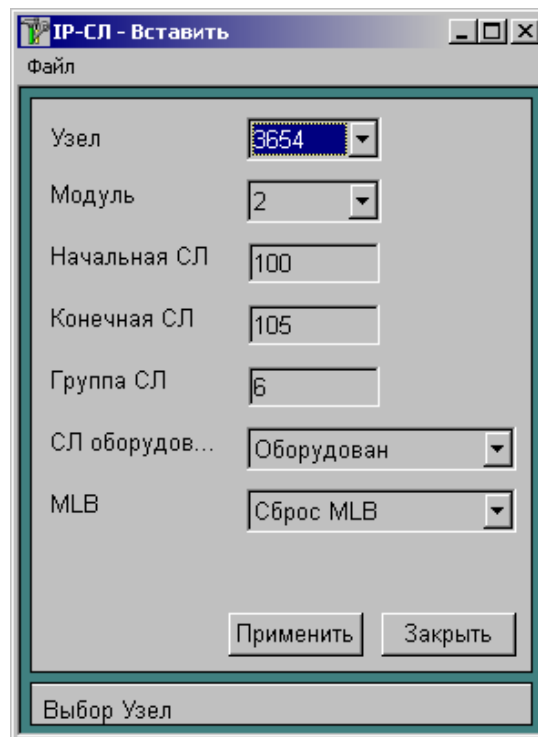


Рис. 3.14 Параметры з'єднувальної IP лінії

3) Після управління сполучними лініями IP вам необхідно управляти сигналізацією, яка буде використовуватися для з'єднання. Для сигналізації, яку ви раніше вибрали для групи з'єднувальних ліній, профіль сигналізації встановлюється адміністративно, і вводиться інформація про віддалену станцію, з якої ви встановлюєте зв'язок (зазвичай інший шлюз IP).

Налаштування сигналізації SIP-T включає в себе процедури

3.1. Адміністрування профілю SIP-T

3.2. Адміністрування віддаленої сторони SIP-T

3.1. Для налаштування властивостей сигналізації SIP-T, які використовуються, коли адмініструються дані для віддаленої сторони обираємо команду CMG > Signalling > SIP-T > Profile

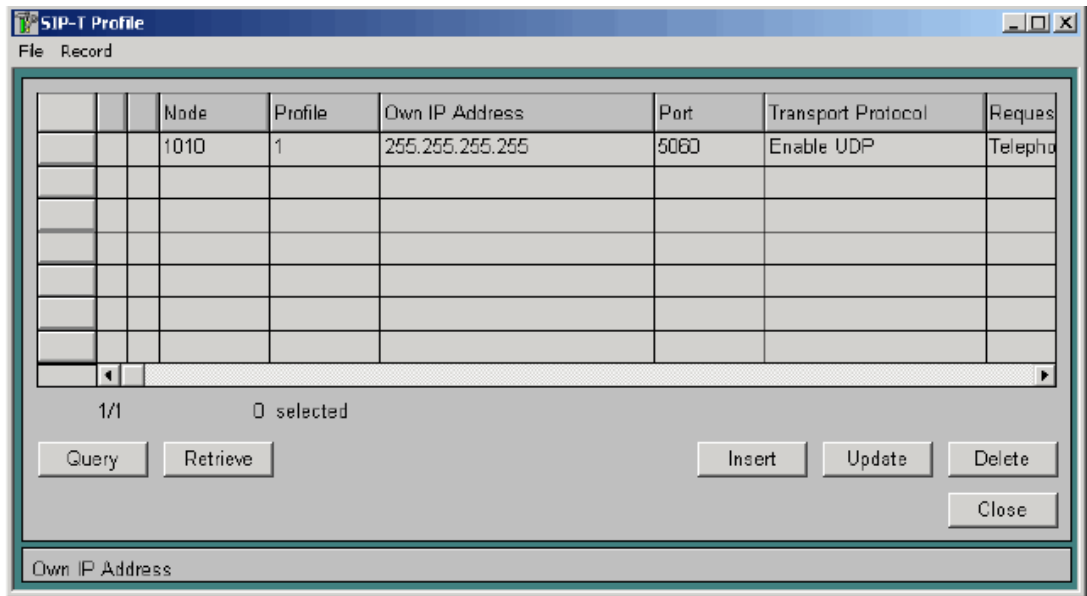


Рис. 3.15 Адміністрування профілей SIP-T

Натискаємо Insert, вписуємо Profile, Request URI

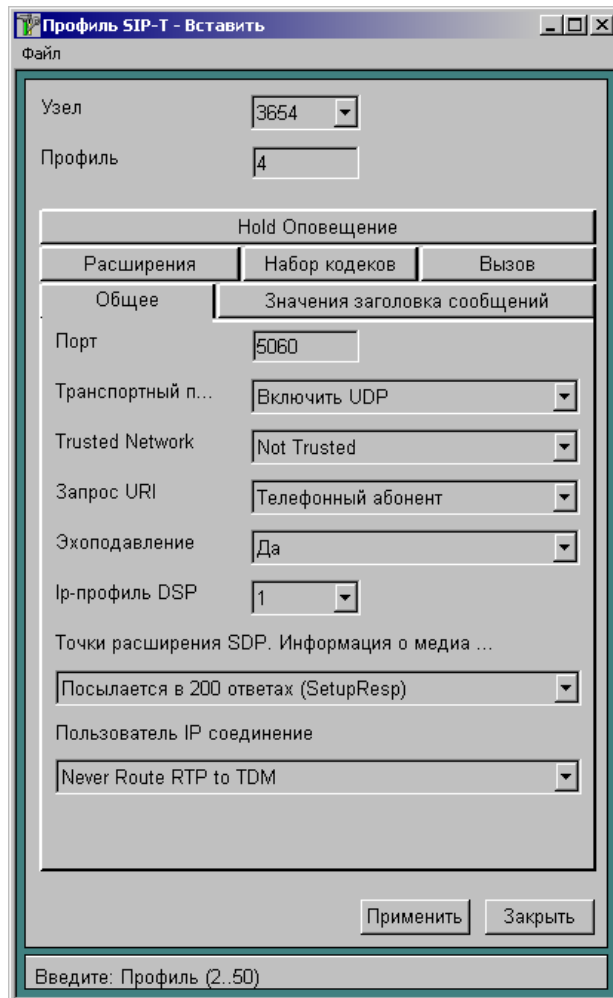


Рис. 3.16 Налаштування профілю SIP-T

3.2 Для адміністрування даних про віддалену сторону, з якої встановлюється комунікація за допомогою сигналізації SIP-T обираємо команду CMG > Signalling > SIP-T > Remote Side.

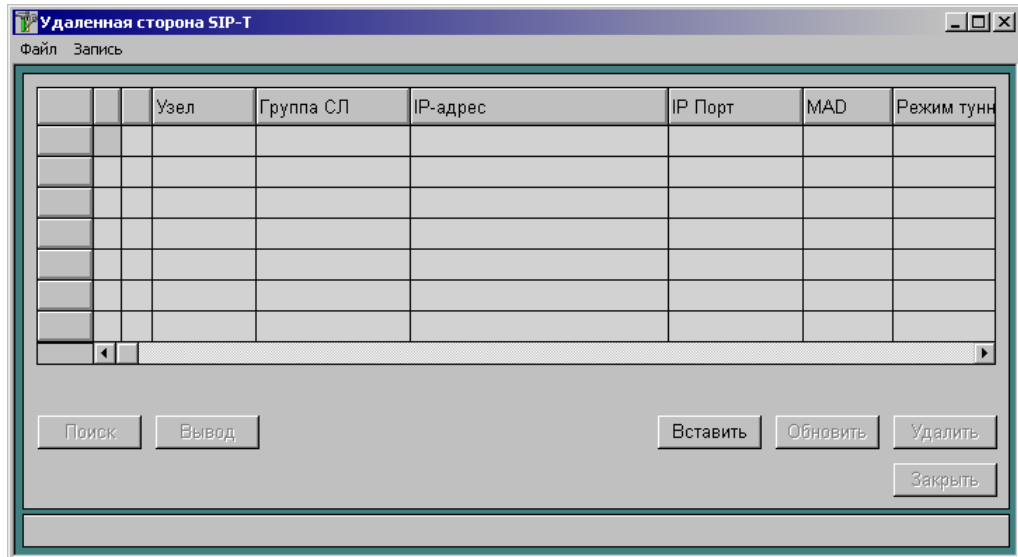


Рис. 3.17 Список параметрів віддаленої сторони

Натискаємо Insert, вписуємо Trunk Group, IP Address, Tunnelling Mode, Profile

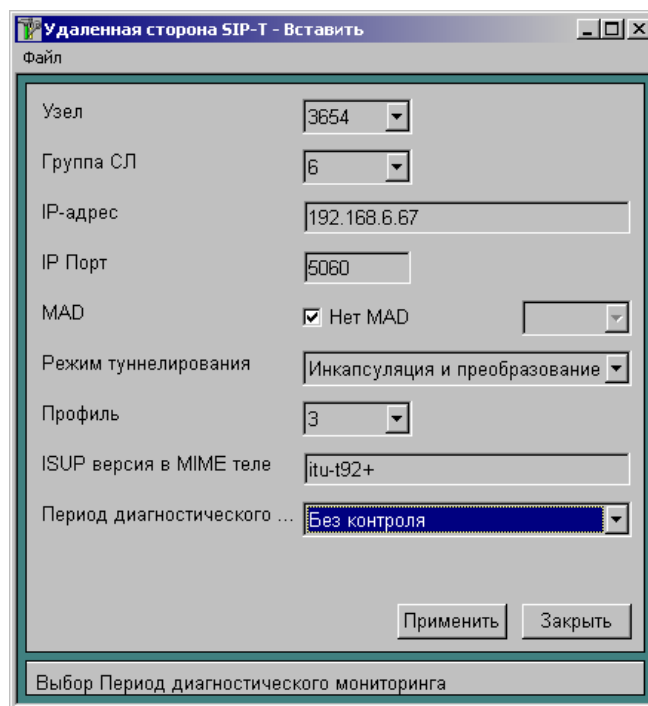


Рис. 3.18 Додаємо параметри серверу з Asterisk

3.2. Налаштування маршрутизації SI2000

Проаналізуємо алгоритм маршрутизації вихідних з'єднань в SI2000

1. В результаті аналізу прийнятих від абонента цифр (префікс-аналізу), визначається номер вихідного пункту призначення (Destination Outgoing).

2. Для кожного вихідного пункту призначення в базі напівпостійних даних визначено один або кілька маршрутних варіантів (Route Seizure Share Variant). Вибір конкретного маршрутного варіанту здійснюється на підставі аналізу таких характеристик виклику, як запитана послуга перенесення інформації (Bearer Service), категорія абонента (Subscriber Category), номер групи входять лінійних комплектів (Incoming Trunk Group), яка обслуговує даний вхідний чи транзитний виклик, і т.д. Умови вибору конкретного маршрутного варіанту заздалегідь описані в базі напівпостійних даних в таблиці Path.

3. Для кожного маршрутного варіанту визначено один або кілька маршрутів (Route). Вибір конкретного маршруту здійснюється за алгоритмом альтернативного вибору або по алгоритму статистичного або тимчасового поділу навантаження.

4. Для кожного маршруту (Route) в базі даних визначена група вихідних або двосторонніх з'єднувальних ліній (Trunk Group), яка використовується для обслуговування даного вихідного дзвінка. Для кожного маршруту може бути визначена тільки одна група сполучних ліній, однак одну і ту ж групу сполучних ліній можуть використовувати кілька маршрутів.

5. Після визначення номера групи з'єднувальних ліній (Trunk Group), система виробляє в цій групі пошук вільної сполучної лінії (Trunk).

6. За номером використовуваної сполучної лінії (Trunk) визначається фізичний номер порту (Port) і каналу (Channel) для обслуговування виклику.

Ознайомимося з схемою порядку створення вихідного маршруту

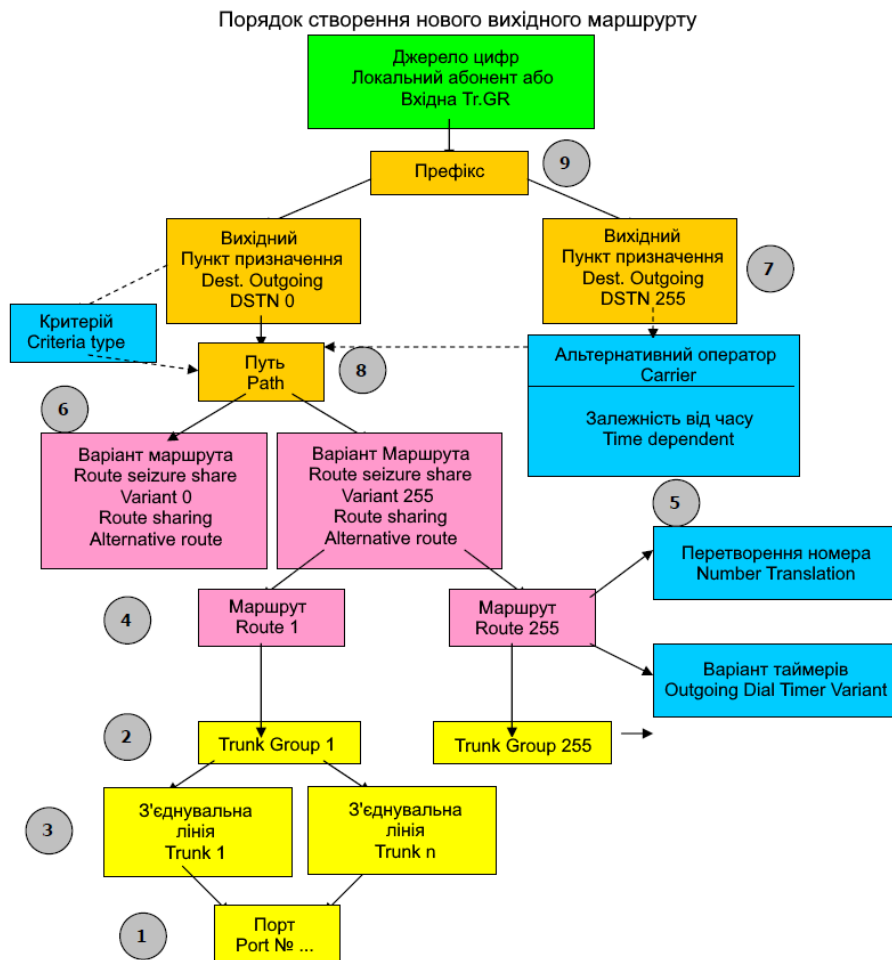


Рис. 3.19 Схема порядку створення вихідного маршруту

Адмініструючи маршрутизацію ви визначаєте спосіб, яким виклики будуть направлятися в IP-мережу. Адміністрування в цілому охоплює адміністрування ланцюжка елементів маршрутизації, які уможливають комунікацію вузла з великим числом вузлів, різні способи поділу трафіку тощо. У випадку, описаному в продовженні, маршрутизація буде відносно простою, оскільки вузол буде з'єднуватися тільки з одним вузлом. Адміністрування маршрутизації охоплює наступні процедури, що виконуються в наступній послідовності:

- 4.1 Адміністрування вихідного пункту призначення;
- 4.2 Адміністрування напрямків;
- 4.3 Адміністрування розподілу трафіку;
- 4.4 Адміністрування шляху;
- 4.5 Адміністрування префіксів.

4.1 Для потреб маршрутизації потрібно перш за все проадмініструвати вихідний пункт призначення обираємо команду CMG > Routing > Destination > Outgoing

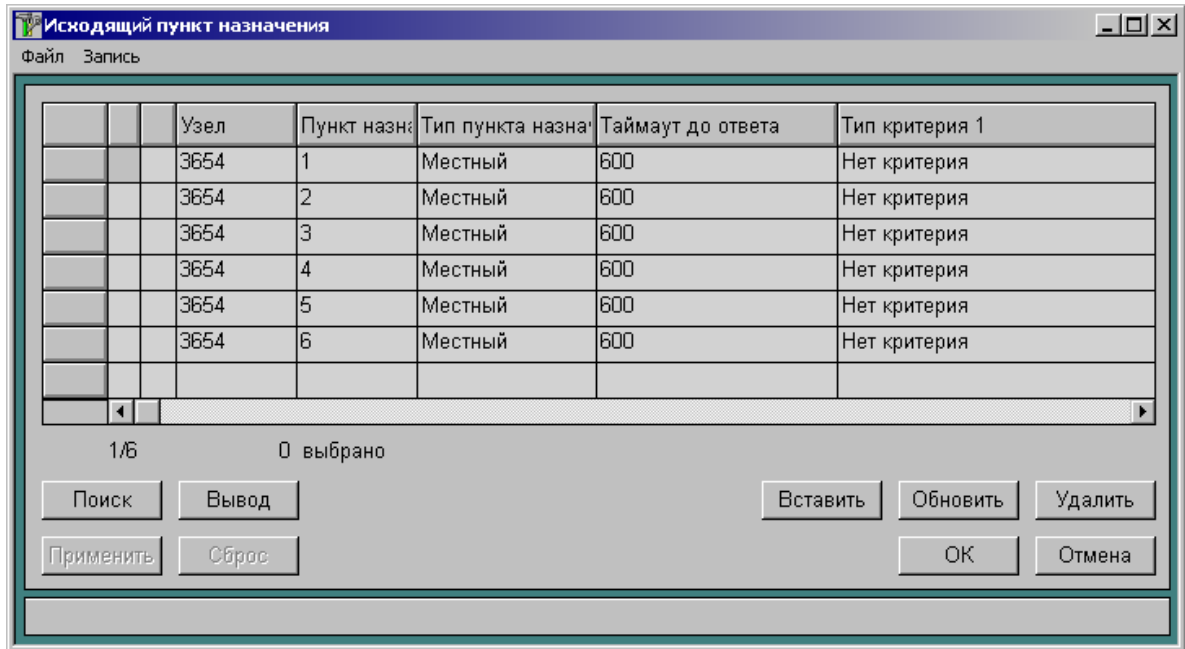


Рис. 3.20 Список віддалених вузлів

Натискаємо Insert, вписуємо Destination, Destination Type.

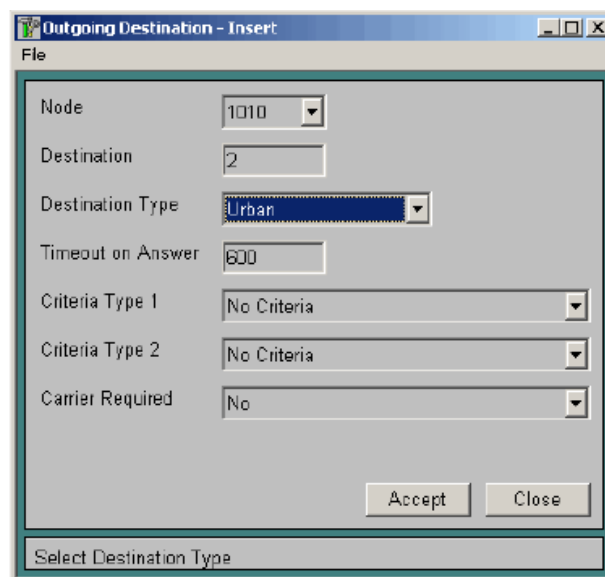


Рис. 3.21 Налаштування віддаленої сторони

4.2 Для налаштування напрямку викликів до вихідного пункту призначення обираємо команду CMG > Routing > Route > Global

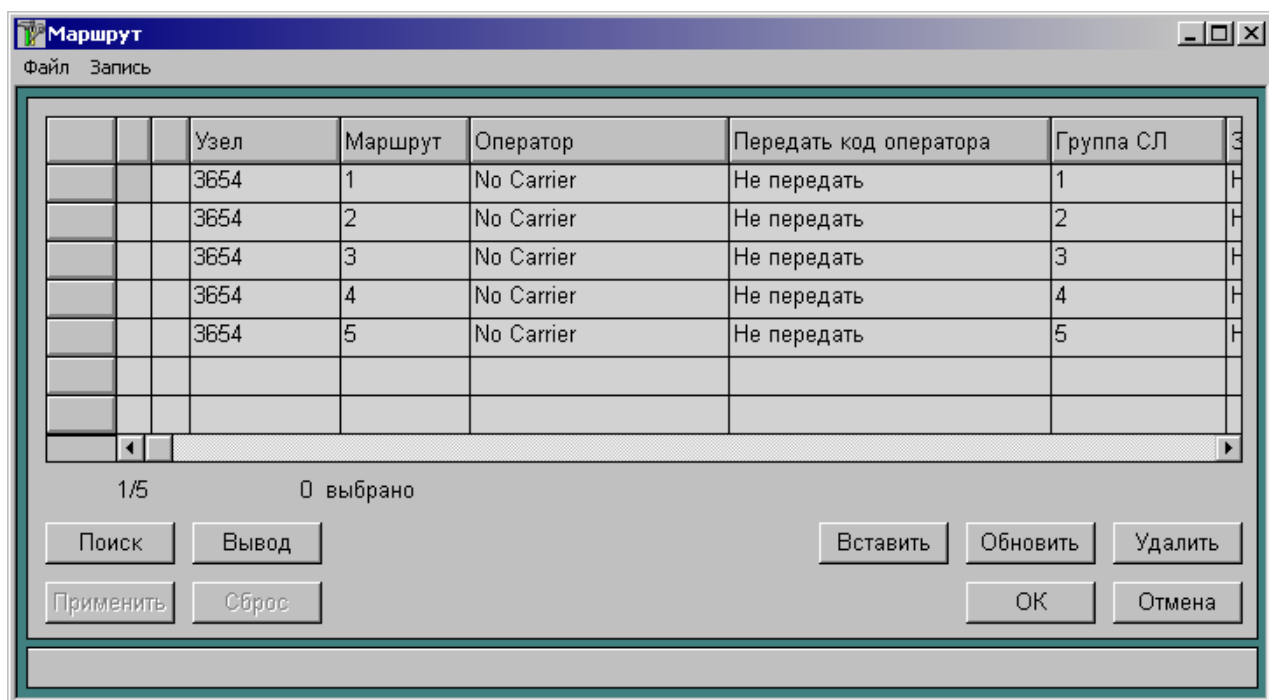


Рис. 3.22 Список маршрутів до вихідного пункту призначення

Натискаємо Insert, вписуємо Route, Trunk Group, Send Digits in Block, First End of Dial Indicator і Outgoing Dial Timer Variant.

Параметри Send Digits in Block, First End of Dial Indicator і Outgoing Dial Timer Variant є важливими для належного функціонування викликів. Send Digits in Block: відправити цифри номера в блоці (виберіть значення Не потрібно, якщо кількість цифр абонентського номера вузла, до якого ви підключені, є фіксованим, або значення. Обов'язково, якщо кількість цифр змінне або у вас немає достовірних даних);

First End of Dial Indicator: перше відображення закінчення набору (введіть значення, яке відповідає сумі цифр коду зони і номера абонента - якщо кількість цифр номера абонента вузла, на якому ви перебуваєте, підключення до змінної, введіть мінімальну кількість позицій);

Outgoing Dial Timer Variant: опція для таймера в вихідному напрямі (введіть значення 0, якщо кількість цифр абонентського номера абонента, з

яким ви з'єднуєтеся фіксоване або значення 1, якщо число цифр змінно або якщо у вас відсутні достовірні дані - в цьому випадку вузол буде перед заняттям напрямку

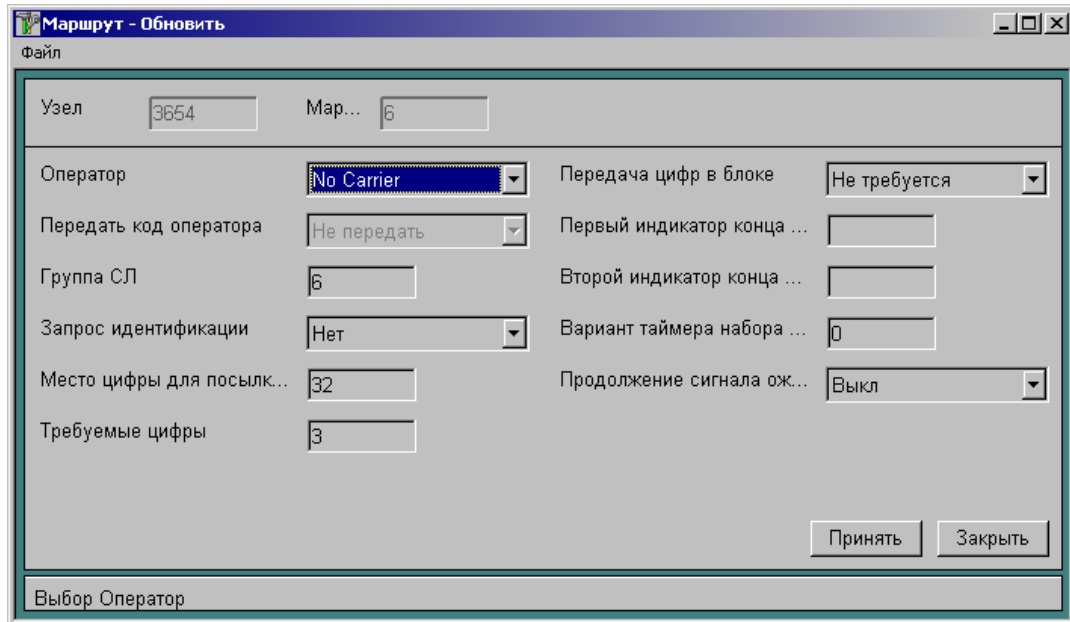


Рис. 3.23 Додаємо маршрут для серверу з Asterisk

4.3 У розподілі трафіку бере участь тільки один напрямок, тобто трафік не ділиться на кілька напрямків. Опція поділу трафіку пов'язує тільки напрямок з маршрутом або вихідними пунктом призначення.

Для налаштування розподілу трафіку обираємо команду CMG > Routing > Route Seizure Share > Variant

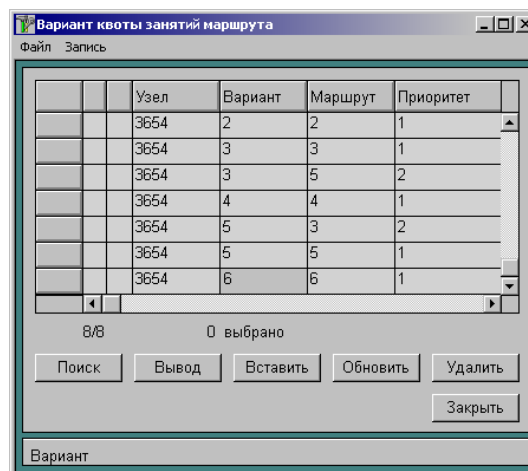


Рис. 3.24 Квоти занять маршруту

Натискаємо Insert, вписуємо Variant, Alternative Routing, Route

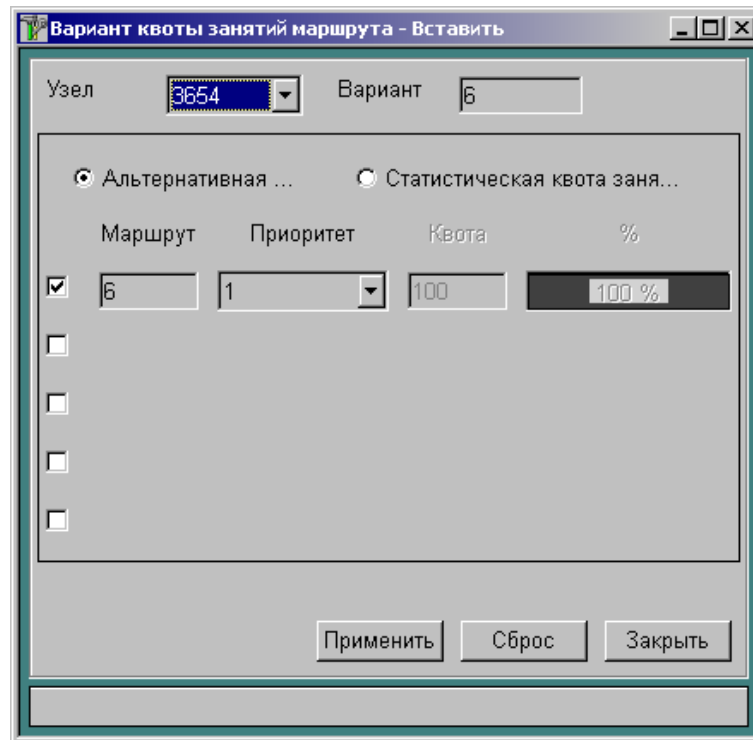


Рис. 3.25 Додаємо опцію розподілу трафіку

4.4 Для аміністрування шляху зв'язуємо пункт призначення та групу з'єднувальних ліній обираємо команду CMG > Routing > Path

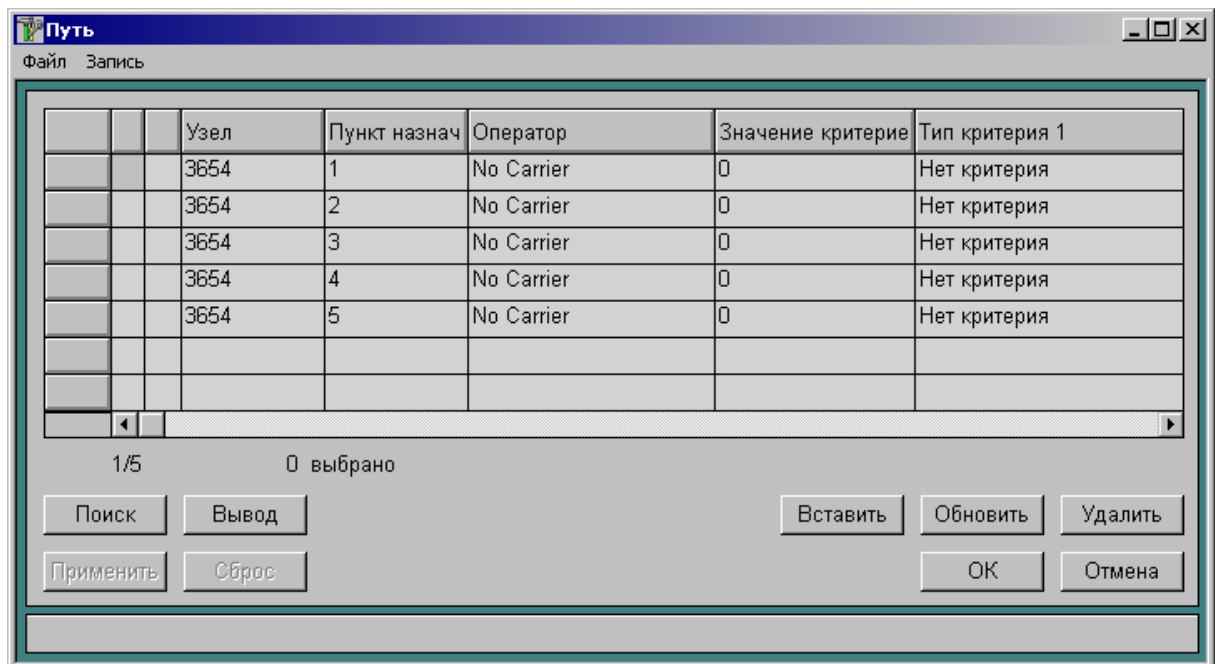


Рис. 3.26 Список пунктів призначення та груп з'єднувальних ліній

Натискаємо Insert, вписуємо Destination, Route Seizure Share Variant

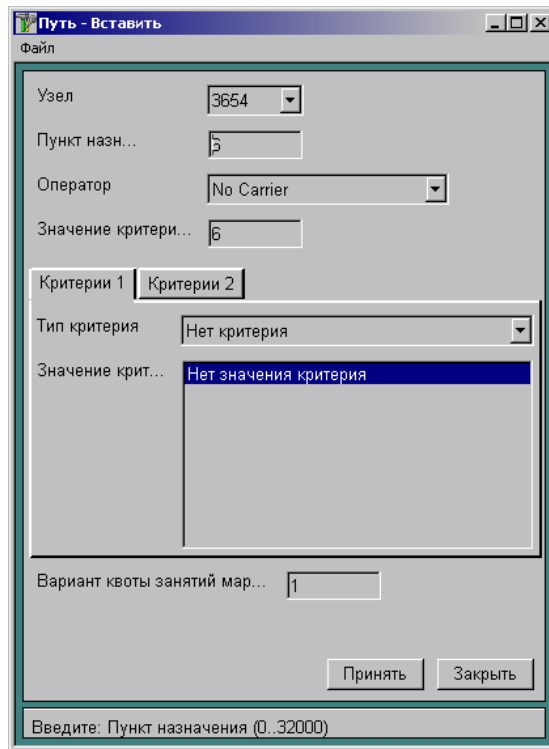


Рис. 3.27 Додаємо потрібний шлях

4.5 Щоб переадресувати виклик іншому вузлу, необхідно визначити перші отримані цифри телефонного номера що викликається. Для налаштування префіксу для посилання на визначене місце призначення вихідного напрямлення обираємо команду CMG > Routing > Prefix.

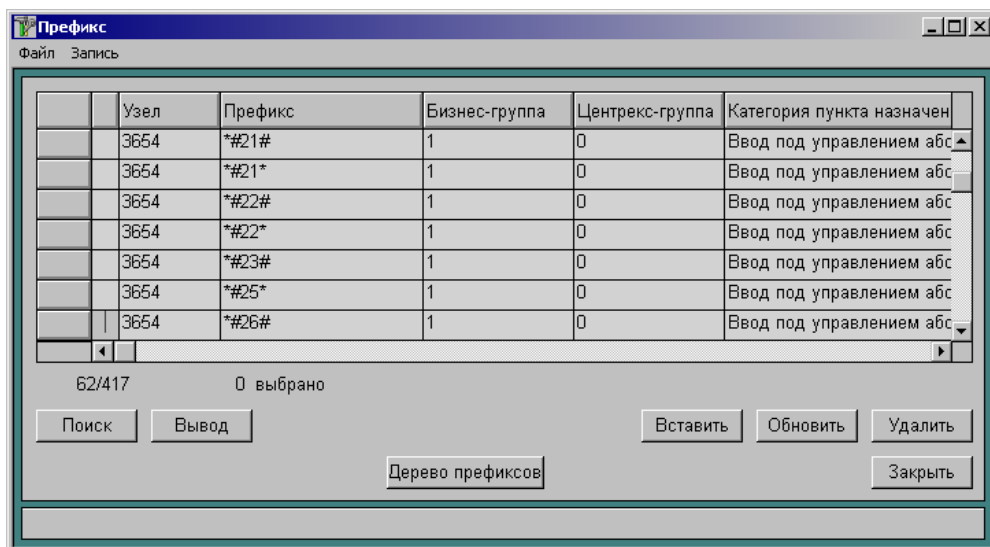


Рис. 3.28 Список префіксів для вибору пункту напрямлення

Натискаємо Insert, вписуємо Prefix, Destination Category, Destination

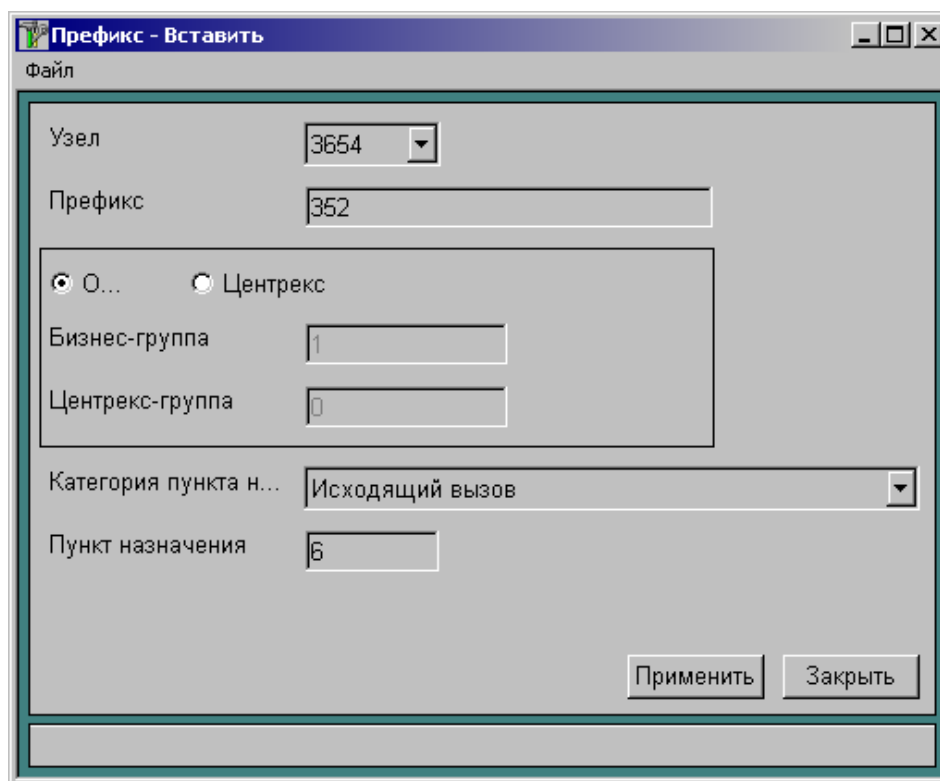


Рис. 3.29 Налаштування префіксу

Останнім кроком в управлінні підключенням IP-шлюзу до IP-мережі є перетворення номерів.

Перетворення номерів необхідно, оскільки номери абонентів (як і ті які викликаються, так і ті які викликають) можуть бути різних типів, значення яких передаються по мережі сигналізації.

Наступні типи номерів можуть бути відправлені в мережу з IP-шлюзом:

- Unknown - код міжміського зони, міжміський код зони і номер абонента (Приклад: 0 4 10000).
- Subscriber - номер учасника (наприклад: 10000). Код національної зони і номер абонента (наприклад: 4 10000).
- International - код міста для міжнародних викликів, код країни, код міста та номер абонента (наприклад: 00 386 4 10000).

Перетворення номерів описується спеціальними параметрами, які складаються з керуючих та інформаційних знаків

Для налаштування перетворення номерів що викликаються в вихідному напрямку обираємо команду CMG > Global > Number Translation > Called – Outgoing

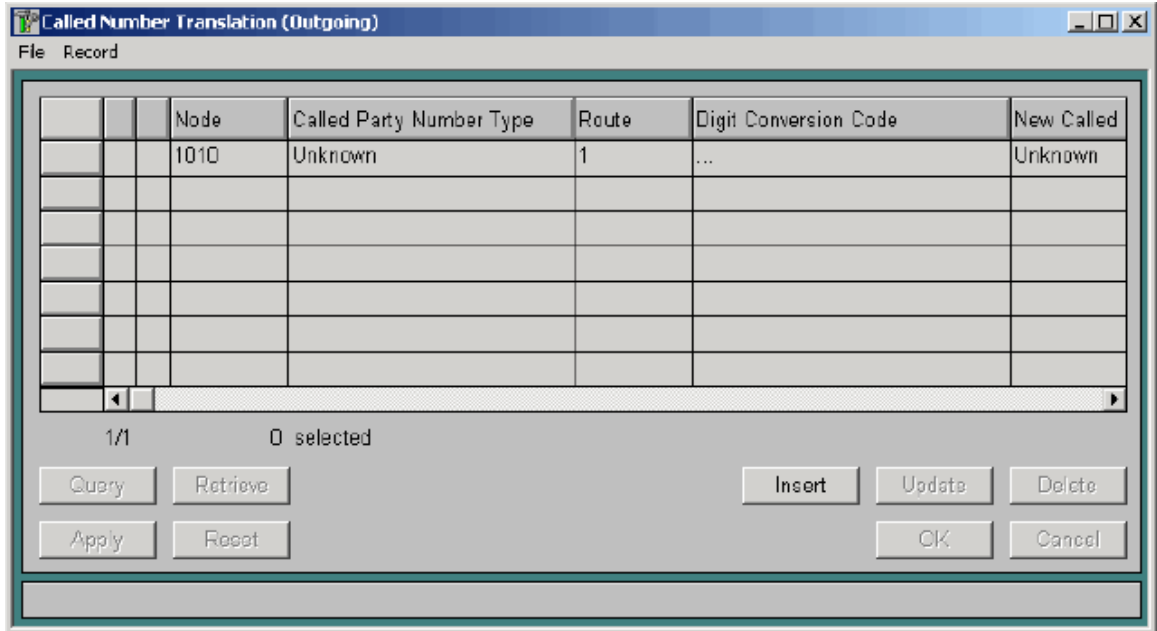


Рис. 3.30 Список налаштувань перетворення номерів що викликаються

Натискаємо Insert, вписуємо Called Party Number Type, Route, Digit Conversion Code, New Called Party Number Type.

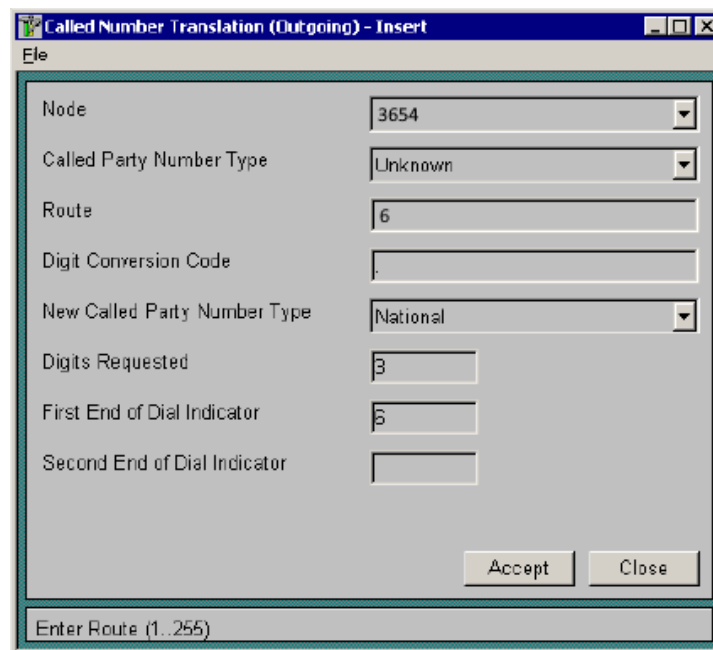


Рис. 3.31 Додаємо параметри перетворення для номеру що викликається

Для налаштування перетворення номерів що викликають в вихідному напрямку обираємо команду CMG > Global > Number Translation > Calling – Outgoing

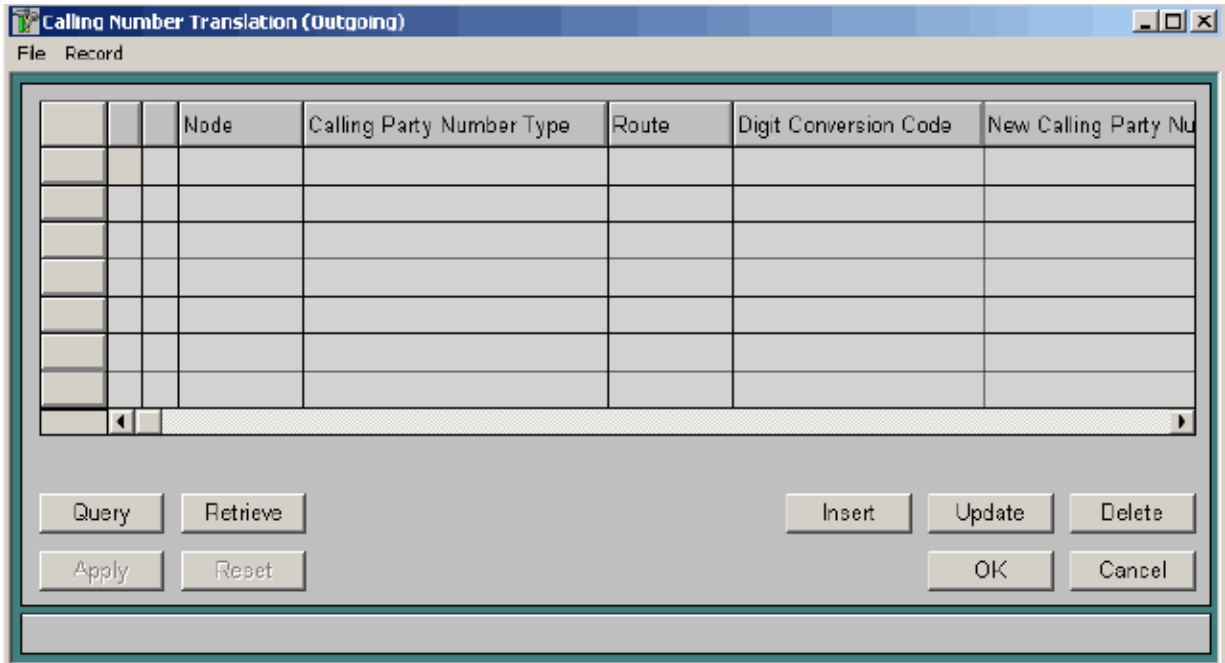


Рис. 3.32 Список налаштувань перетворення номерів що викликають

Натискаємо Insert, вписуємо Called Party Number Type, Route, Digit Conversion Code, New Called Party Number Type.

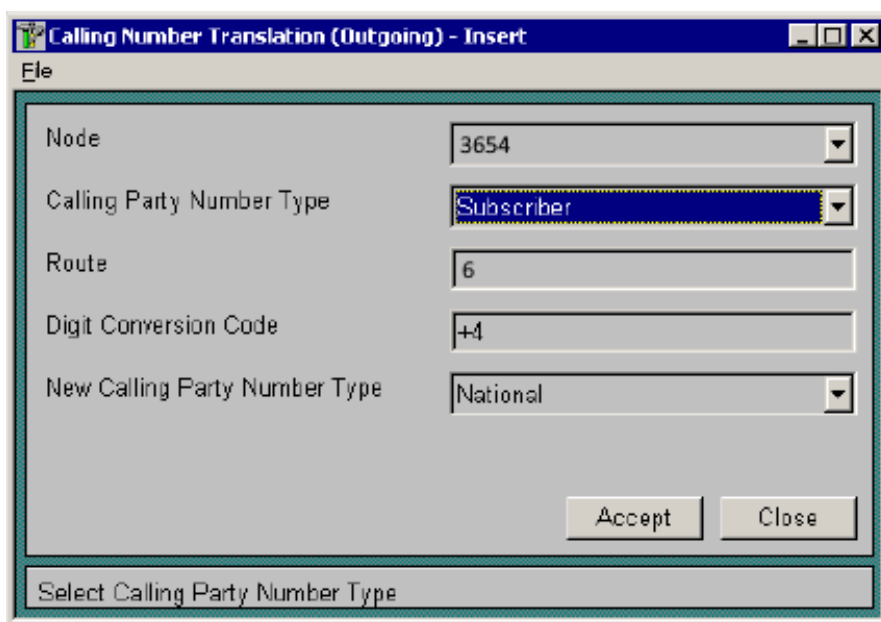


Рис. 3.33 Додаємо параметри перетворення для номеру що викликає

3.3. Встановлення та налаштування Asterisk 13

Для побудови каналу зв'язку АТС SI2000 з Asterisk, для початку потрібно встановити та коректно сконфігурувати ПЗ Asterisk.

3.3.1. Встановлення Asterisk 13

Для встановлення Asterisk 13 буде використано дистрибутив CentOS7

Виконуємо команди у такому порядку

Вказуємо DNS Server:

```
echo 'nameserver 8.8.8.8' >> /etc/resolv.conf
```

Встановлюємо додатковий репозиторій:

```
yum -y install epel-release
```

Встановлюємо необхідні утиліти:

```
yum -y install gcc-c++ ncurses-devel libxml2-devel wget openssl-devel newt-  
devel kernel-devel-`uname -r` sqlite-devel libuuid-devel gtk2-devel jansson-devel  
binutils-devel bzip2 patch libedit libedit-devel
```

Відключаємо SELINUX:

```
sed -i 's/SELINUX=enforcing/SELINUX=disabled/g' /etc/selinux/config  
setenforce 0
```

Оновлюємо пакети системи до найбільш актуальних:

```
yum -y update
```

Перезавантажуємо систему:

```
reboot
```

Переходимо в каталог, куди будемо скачувати архів:

```
cd /usr/src/
```

Скачуємо архів:

```
wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-13-  
current.tar.gz
```

Розпаковуємо архів:

```
tar xzvf asterisk-13-current.tar.gz
```

Переходимо в каталог з вихідними файлами:

```
cd asterisk-13.*
```

Виконуємо скрипт для встановлення пакетів с залежностями Asterisk

```
contrib/scripts/install_prereq install
```

Виконуємо команду:

```
./configure --libdir=/usr/lib64 --with-jansson-bundled
```

Налаштовуємо конфігурацію:

```
make menuselect
```

Відмічаємо модулі які потрібно встановити

```
save & exit
```

Компілюємо ПЗ:

```
make && make install
```

Створюємо конфігурацію для запуску Asterisk:

```
make config
```

Створюємо стандартні конфігурації:

```
make samples
```

Запускаємо Asterisk:

```
/etc/init.d/asterisk start
```

Включаємо автоматичний запуск Asterisk:

```
systemctl enable asterisk
```

3.3.2. Налаштування каналу зв'язку на Asterisk

Налаштування каналу зв'язку виконується в файлі `/etc/asterisk/sip.conf`.

Лістинг налаштувань з'єднувальної лінії:

```
[SI2000]
type=friend
insecure=port,invite
host=192.168.6.101
port=5060
disallow=all
allow=ulaw
allow=alaw
directmedia=no
canreinvite=no
context=si2000_test
qualify=yes
description=SI2000
```

Рис. 3.34 Лістинг налаштувань з'єднувальної лінії

Виконуємо команду rasterisk -x 'sip show peers' для того щоб перевірити коректність лістингу та наяву каналу зв'язку з SI2000

```
[root@localhost asterisk-13.38.2]# rasterisk -x 'sip show peers'
Name/username      Host                               Dyn Forcerport Comedia  ACL Port  Status  Description
SI2000             192.168.6.101                     Auto (No)  No        5060     OK (11 ms) SI2000
1 sip peers [Monitored: 1 online, 0 offline Unmonitored: 0 online, 0 offline]
```

Рис. 3.35 Результат команди rasterisk -x 'sip show peers'

Як бачимо зі скріншоту вище канал зв'язку з АТС SI2000, АТС доступна та готова передавати або приймати виклики.

3.3.3. Налаштування маршрутизації на Asterisk

Налаштування маршрутизації виконується в файлі
/etc/asterisk/extensions.conf

Лістинг налаштувань маршрутизації дзвінка з SI2000

```

[si2000_test]
exten => _X.,1,NoOp(${CALLERID(all)})
same=> n,GoSub(number-normalize-long_numbers,${EXTEN},1)
same=> n,Answer()
same=> n,Playback(Playback_394875)
same=> n,Macro(queue,9)
same=> n,Hangup()

[number-normalize-long_numbers]
exten => _X.,1,NoOp()
same=> n,AGI(normalize.sh,${CALLERID(num)},{CHANNEL})
same=> n,Noop(${normalized})
same=> n,Set(dialednumber=${EXTEN})
same=> n,Set(caller=${normalized})
same=> n,Set(CALLERID(name)=${caller})
same=> n,Set(CALLERID(num)=${caller})
same=> n,Macro(blacklist,${CALLERID(num)})
same=> n,Return()

[macro-queue]
exten => s,1,Answer()
same => n,Noop(Result QUEUE, GOTO QUEUE)
same => n,Set(VIP=${ODBC_VIP(${CALLERID(num):-10}})})
same => n,ExecIf(["${VIP}" = ""]?Set(VIP=${ODBC_VIP(${CALLERID(name):-10}})))
same => n,GotoIf(["${VIP}" = "1"?viip,s,1)
same => n,GotoIf(["${VIP}" = "2"?viip,s,1)
same => n,AgI(agi://${AGIIP}/Queue?queueId=${ARG1})
same => n,MacroExit()

[viip]
exten => s,1,NoOp(vip)
same => n,AgI(agi://${AGIIP}/Queue?queueId=7)
same => n,MacroExit()

```

Рис. 3.36 Лістинг налаштувань маршрутизації

ВИСНОВКИ ДО РОЗДІЛУ 3

У даному розділі було проведено налаштування та тестування системи телефонії на базі Asterisk та серверу CentOS. Під час тестування було виявлено переваги даного комплексу в порівнянні з SI2000:

- Набагато легше налаштування
- Поширеність системи телефонії на базі Asterisk в наслідок чого велика кількість інформації щодо використання та налаштування.

ВИСНОВКИ

Метою дипломної роботи було побудувати канал зв'язку між цифровою АТС SI2000 та IP АТС Asterisk. А також використання цифрової АТС SI2000 в якості шлюза IP-мережі.

У першому розділі дипломної роботи було розглянуто поняття Internet Protocol, різні категорії IP-адрес такі як: споживчі IP-адреси, приватні IP-адреси, загальнодоступні IP-адреси. Також те що загальнодоступні IP-адреси бувають двох видів - динамічні та статичні. Динамічні IP-адреси змінюються автоматично і регулярно, а статичні IP-адреси залишаються незмінними. Було проаналізовано поняття IP-телефонія - це термін, що використовується для опису технологій, що використовують різноманітні протоколи для обміну голосом, факсом, іншими формами інформації та були знайдені відміни від поняття VoIP. VoIP - це передача голосу та мультимедійного вмісту через Інтернет. Проаналізовані основні протоколи VoIP та детально розглянуті протоколи SIP та H.323, їх переваги та недоліки, принципи роботи та актуальність використання цих протоколів на сьогоднішній день. Основна різниця полягає в тому що H.323 не дуже підходить для управління голосом через IP-системи, за своєю суттю є складним, має накладні розходи, не має розширюваності, використовує двійкове представлення для своїх повідомлень, не дуже масштабований та обмежений при виконанні виявлення циклу в складних багатодоменних пошуках.

У другому розділі дипломної роботи було розглянуте основне обладнання що використовуються для VoIP, такі як: IP АТС, Шлюз VoIP (аналоговий, цифровий, шлюзи GSM SIP), IP-маршрутизатор, аналоговий телефонний адаптер, IP-телефон (апаратні та програмні). Розглянуто та порівняно основні кодеки VoIP, а саме: G711, G722, GSM, G729. Було розглянуто основні переваги IP-АТС Asterisk (відкрита комунікаційна

платформа, котра використовується для розгортання програмних АТС, систем голосового зв'язку, VoIP-шлюзів, організації IVR-систем, голосової пошти, телефонних конференцій і call-центрів) та цифрової АТС ISKRATEL SI2000 (сучасної цифрової комутаційної системи з керуванням по записаній програмі, призначена для використання на ТМЗК). Було проаналізована функціональна схема станції та основні характеристики станції.

У третьому розділі дипломної роботи було конфігурування іCS SI2000 з функціями IP-шлюзу, а саме: налаштування мережевого IP-з'єднання, налаштування інтерфейса Ethernet, управління IP-адресами для підключення, управління сполучними лініями IP (адміністрування модуля IP, адміністрування групи з'єднувальних ліній IP, внесення сполучних ліній IP), налаштування групи з'єднувальних ліній IP, внесення сполучних ліній IP, налаштування сигналізації SIP-T (адміністрування профілю SIP-T, адміністрування віддаленої сторони SIP-T), налаштування властивостей сигналізації SIP-T для віддаленої сторони, адміністрування даних про віддалену сторону, з якої встановлюється комунікація за допомогою сигналізації SIP-T. Було налаштовано маршрутизацію, а саме, адміністрування вихідного пункту призначення, адміністрування напрямків, адміністрування розподілу трафіку, адміністрування шляху, адміністрування префіксів. Проаналізовано параметри Send Digits in Block, First End of Dial Indicator і Outgoing. Також було встановлено та сконфігуровано IP АТС Asterisk, було проведено налаштування каналу зв'язку на Asterisk та налаштування маршрутизації на Asterisk.

Отже канал зв'язку був побудований між АТС SI2000 та IP АТС Asterisk і тепер можна використовувати переваги обох технологій: надійність та сумісність з застарілими технологіями та високу якість зв'язку, мобільність, розширений функціонал, низька вартість передачі даних та простота експлуатації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. <https://www.techopedia.com/definition/26128/ip-network>
2. <https://www.kaspersky.com/resource-center/definitions/what-is-an-ip-address>
3. <https://www.nextiva.com/blog/what-is-ip-telephony.html>
4. https://www.cse.wustl.edu/~jain/cis788-99/ftp/voip_protocols/
5. <https://getvoip.com/blog/2020/10/27/voip-equipment>.
6. <https://ru.wikipedia.org/wiki/IP-%D0%90%D0%A2%D0%A1>
7. <https://new-tel.net/blog/voip-shlyuz-hto-eto-takoe-i-kak-ego-vybrat-biznesu/>
8. <https://wiki.merionet.ru/ip-telephoniya/5/voip-codecs/>
9. <https://www.icepartners.ru/blog/20-stati/627-polosa-propuskaniya-ispolzuemaya-v-voip.html>
10. <https://www.asterisk.org/get-started/applications/gateway/>
11. <https://searchunifiedcommunications.techtarget.com/definition/VoIP>
12. <https://uk.wikipedia.org/wiki/Asterisk>
13. <https://www.asterisk.org/get-started/>
14. [https://www.iskratel.com/si/-LS5092 – B – System Description](https://www.iskratel.com/si/-LS5092-B-System-Description)
15. [https://www.iskratel.com/si/-LS5092 – C – Getting Started](https://www.iskratel.com/si/-LS5092-C-Getting-Started)