

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Тернопільський національний економічний університет
Факультет комп'ютерних інформаційних технологій
Кафедра комп'ютерної інженерії

Соловій Олена Михайлівна

**Корпоративна телефонна мережа VoIP з використанням
програмного забезпечення Asterisk / Corporate VoIP
telephone network based on Asterisk software**

напрямок підготовки: 6.050102 - Комп'ютерна інженерія
фахове спрямування - Комп'ютерні системи та мережі
Бакалаврська робота

Виконав студент групи КСМз-41/2
О.М. Соловій

Науковий керівник:
Вербовий С.О.

Тернопіль - 2018

РЕЗЮМЕ

Дипломний проект містить 81 сторінку пояснюючої записки, 25 рисунків, 8 таблиць та 2 додатки. Обсяг графічного матеріалу 2 аркуші формату А3.

Метою проекту є розробка корпоративної мережі VoIP з використанням програмного забезпечення Asterisk.

Актуальність розвитку КТМ на основі IP-телефонії обумовлена не тільки можливістю зниження витрат на телефонні переговори і технічне обслуговування інфраструктури. У стратегічному плані IP-телефонія є єдиною технічною платформою, яка дозволить об'єднати рішення для передачі даних і голосу, а також для обробки і подальшого використання цієї інформації у всіх бізнес-процесах.

В першому розділі дипломного проекту проведено аналіз основних підходів до створення КТМ. Досліджено компоненти та протоколи IP-телефонії.

Другий розділ присвячений вибору протоколу для впровадження IP-телефонії. Приведено архітектуру мережі SIP та описано методи забезпечення якості обслуговування.

У третьому розділі описано метод сполучення VoIP-мережі з ТМЗК. Наведено приклад налаштування Asterisk-сервера на OS Linux. Проведено моделювання та перевірку спроектованої телефонної мережі

У четвертому розділі проведено економічні розрахунки.

Ключові слова: VoIP, КТМ, IP-телефонія, ТМЗК, Asterisk.

RESUME

The diploma project contains 81 pages of the explanatory note, 25 figures, 8 tables and 2 annexes. The volume of graphic material is 2 sheets of A3 format.

The goal of the project is to develop a corporate VoIP network using the Asterisk software.

The urgency of the development of KTM on the basis of IP-telephony is due not only to the possibility of reducing the cost of telephone negotiations and maintenance of infrastructure. In the strategic plan, IP telephony is the only technical platform that will combine solutions for data and voice, as well as for processing and further use of this information in all business processes.

In the first section of the diploma project, an analysis of the main approaches to the creation of a CTN. The components and protocols of IP telephony are investigated.

The second section is devoted to the choice of protocol for the implementation of IP telephony. The architecture of the SIP network is described and methods of providing quality of service are described.

The third section describes the method of connecting a VoIP network to a TCPC. Here is an example of how to configure the Asterisk server on OS Linux. Modeling and testing of the designed telephone network was carried out

The fourth section provides economic calculations.

Keywords: VoIP, CTN, IP-telephony, TNGU, Asterisk.

ЗМІСТ

Вступ.....	9
1 Теоретичний огляд підходів до побудови КТМ.....	10
1.1 Основна мета та порівняння підходів до створення КТМ	10
1.2 Компоненти IP-телефонії	15
1.3 Протоколи мереж IP-телефонії	17
1.4 Постановка задачі.....	26
2 Проектування мережі передачі голосу.....	27
2.1 Вибір протоколу IP-телефонії.....	27
2.2 Архітектура мережі SIP	33
2.3 Методи забезпечення якості обслуговування	37
3 Реалізація корпоративної телефонної мережі	45
3.1 Рішення для телефонної мережі філії	45
3.2 Сполучення VoIP-мережі з ТМЗК.....	49
3.3 Налаштування Asterisk-сервера на ОС Linux	50
3.4 Моделювання телефонної мережі компанії.....	55
3.5 Перевірка працездатності мережі	62
4 Техніко-економічний розділ	65
4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи	65
4.2 Розрахунок ціни проекту	71
4.3 Визначення економічної ефективності і терміну окупності капітальних ...	72
вкладень.....	72
Висновки	74
Список використаних джерел.....	75
Додаток А Команди налаштування Asterisk та FreePBX	Помилка! Закладку не визначено.
Додаток Б Довідка про використання	Помилка! Закладку не визначено.

					ДП.КСМ.111862/16.00.00.000 ПЗ			
Змн.	Лист	№ докум.	Підпис	Дата				
Розробив	Соловій О.М				КОРПОРАТИВНА ТЕЛЕФОННА МЕРЕЖА VOIP 3 ВИКОРИСТАННЯМ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ASTERISK	Літ.	Арк.	Акрушів
Перевір.	Вербовий С.О.						8	81
Консульт.	Паздрій І.Р.					ТНЕУ. ННІОТ. КСМзкп-41/2		
Н. Контр.	Гурадь І.В.							
Затвердив	Березький О.М							

ВСТУП

Кількість IP-користувачів швидко зростає, тому і розширюються можливості IP-мереж. Поряд із передачею даних їх також можна використовувати для інтерактивних відеоконференцій, передачі потоків голосової інформації та для інших додатків реального часу.

Практична можливість повної інтеграції голосу і даних поверх загальної інфраструктури обчислювальних мереж привела до появи так званої «пакетної телефонії» - технології передачі аналогових телефонних сигналів по мережах передачі даних.

В IP-телефонії використовується технологія, що дозволяє використовувати будь-яку мережу з пакетною комутацією на базі протоколу IP, як засобу організації і ведення міжнародних, міжміських і місцевих телефонних розмов та передачі факсів в режимі реального часу.

Створення корпоративної телефонної мережі (КТМ) є обов'язковим вирішальним кроком для створення гнучкої динамічної телекомунікаційної інфраструктури, яка дозволить швидко організовувати та динамічно підтримувати сучасні колективи та робочі групи, організовувати як внутрішній зв'язок, так і зовнішню взаємодію.

Актуальність розвитку КТМ на основі IP-телефонії обумовлена не тільки можливістю зниження витрат на телефонні переговори і технічне обслуговування інфраструктури. У стратегічному плані IP-телефонія є єдиною технічною платформою, яка дозволить об'єднати рішення для передачі даних і голосу, а також для обробки і подальшого використання цієї інформації у всіх бізнес-процесах.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						9
Змн.	Арк.	№ докум.	Підпис	Дата		

1 ТЕОРЕТИЧНИЙ ОГЛЯД ПІДХОДІВ ДО ПОБУДОВИ КТМ

Під корпоративною телефонною мережею (КТМ) розуміється сектор телекомунікації, що забезпечує сучасний телефонний сервіс (внутрішні, зовнішні і міжміські переговори, аудіо та відео конференції, передачу повідомлень, голосову пошту і т.п.) для абонентів.

Такі телефонні мережі можуть об'єднувати велику кількість абонентів на всіх територіях окремого підприємства. Вони можуть бути складно зв'язані і покривати місто, країну або навіть всю земну кулю.

1.1 Основна мета та порівняння підходів до створення КТМ

Вибираючи на користь того чи іншого рішення, необхідно орієнтуватися не тільки на вартість, але також виходити з функціональних потреб організації.

КТМ мають можливість надавати такі телефонні сервіси:

- внутрішній корпоративний телефонний сервіс - внутрішня оптимізована за витратами і єдина по нумерації телефонна мережа абонентів;
- міжміський телефонний зв'язок з використанням корпоративних каналів СПД;
- доступ до альтернативного оператора міжнародного, міжміського телефонного зв'язку, що дозволяє знизити затрати на оплату телефонних переговорів;
- корпоративне підключення до операторів мобільного зв'язку;
- доступ до студій проведення корпоративних відео конференцій.

Актуальність створення КТМ обумовлена двома факторами. З одного боку, існуючий парк внутрішніх АТС вичерпав свій технологічний ресурс і вимагає заміни, з іншого – наявність телекомунікаційної внутрішньої інфраструктури

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						10
Змн.	Арк.	№ докум.	Підпис	Дата		

дозволяє застосовувати сучасні комунікаційні рішення, використовуючи власні ресурси, а не купуючи сервіси у традиційних операторів.

Таким чином, виникла можливість істотно розширити сферу застосування СПД, використовуючи її не тільки для передачі даних, але і для організації аудіо та відео трафіку.

Існує кілька підходів реалізації корпоративних телефонних мереж.

Основними послугами крім скороченого набору номера і тристороннього конференц-зв'язку, є:

- перевід з'єднання на телефонний номер третього абонента (Call Transfer);
- переадресація вхідних дзвінків на інший, заздалегідь заланий номер в межах CUG (Call Forwarding);
- перехоплення викликів, що надходять до абонентів CUG (Call Pick-up);
- повідомлення про виклик, що надійшов в стані розмови (Call Waiting);
- утримання виклику, його перемикання в стані розмови з одного з'єднання на інше (Call Hold);
- встановлення з'єднання з зайнятим абонентом після його звільнення (Call Back);
- прямий виклик (Hot Line).

Перераховані послуги вигідні і для операторів мереж, оскільки є джерелом додаткових доходів, а також ефективним засобом зменшення числа невдалих спроб встановлення з'єднань. Однак, як і в будь-якої системи є ряд недоліків.

На сьогоднішній день існує два основних шляхи створення власної КТМ. Першим є придбання власного телефонного обладнання - уніфікованої автономної телефонної станції (УАТС) і підключення її до телефонної мережі загального користування (ТМЗК). Таке підключення може бути зроблено за допомогою аналогових абонентських ліній або за допомогою підключення по потоку Е1. У разі аналогового підключення кількість виділених оператором ТМЗК номерів дорівнює кількості ліній. Даний варіант підключення прийнятний тільки для офісних міні-АТС, але не може в повній мірі задовольнити потреби корпоративного клієнта, так як число абонентів в мережі може обчислюватися

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		11

сотнями, в деяких випадках тисячами, до того ж це стає неефективним з економічної точки зору. Оренда цифрового потоку, навпаки, нерентабельна для невеликих організацій із-за неможливості раціонально використовувати всю його ємність.

Функції сучасних УАТС можна розділити на наступним групи. В першу, безсумнівно, входять базові телефонні функції, включають встановлення з'єднань всередині станції і з зовнішніми абонентами. До інтелектуальних функцій обробки викликів можна віднести переадресацію, скорочений набір, утримання і перехоплення викликів, автонабір, конференцзв'язок і багато іншого. УАТС із можливостями ISDN широко підтримують функції передачі даних, відеоконференц-зв'язок і сполучення з локальними мережами та корпоративними інформаційними системами [1].

Важливу роль відіграють питання інформаційної безпеки компанії, адже забезпечити конфіденційність набагато простіше, якщо телефонна станція контролюється самою компанією.

Другим і більш вигідним з економічної точки зору варіантом розвитку КТМ, є побудова мережі на базі технології VoIP, але при цьому важливим елементом такої мережі є наявність існуючої ЛОМ і/або СПД.

Перехід на IP-технології при побудові корпоративних телефонних мереж має певні переваги. В першу чергу пакетна телефонія дозволяє істотно економити необхідну смугу пропускання каналів, що неминуче веде до зниження тарифів, особливо на міжміські і міжнародні телефонні розмови, що є привабливим, як для операторів, так і для корпоративних клієнтів.

По-друге використання єдиної кабельної інфраструктури для мереж передачі даних і телефонії. При цьому скорочується кількість кабелів, так як IP-телефони співробітників і їх персональні комп'ютери підключаються до однієї розетки. Такий варіант забезпечується комутатором, вбудованим в сам телефонний апарат.

У корпоративній мережі IP-телефонії кожному апарату присвоюється унікальна IP-адреса в рамках прийнятої адресації. Ця адреса може призначатися

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		12

адміністратором мережі або автоматично за допомогою протоколу DHCP. Більшість апаратів разом з IP-адресою можуть отримувати від DHCP-сервера інформацію про джерело індивідуальних файлів конфігурації і, при необхідності, нові версії програмного забезпечення (Firmware). Такий підхід спрощує обслуговування абонентів в порівнянні з традиційними телефонними системами. Відпадає необхідність комутувати щось на кросі, наприклад, при переїзді абонента в іншу кімнату – досить включити апарат в розетку.

Перше покоління систем корпоративної IP-телефонії мали, з точки зору зручності експлуатації, один істотний недолік - вони вимагали місцевого електроживлення. Зараз знайдено рішення цієї проблеми - виробники активного мережного обладнання стали пропонувати моделі комутаторів, що забезпечують дистанційне живлення IP-телефонів по Ethernet-проводці (PoE) і більшість моделей IP-телефонів також підтримують живлення за стандартом IEEE 802.3af. Крім дорогих комутаторів з підтримкою PoE деякі виробники пропонують багатопортові інжектори живлення PoE за розумними цінами.

Сучасні системи корпоративної IP-телефонії підтримують всі основні сервісні функції УАТС. Однак головним перевагою корпоративної IP-телефонії, що робить її популярною в очах абонентів, є нові види сервісу, реалізація яких на базі традиційних УАТС була складною. Прикладом може служити універсальний операторський центр, пов'язаний з Web-сайтом електронної комерції компанії. Завдяки протоколу IP інтеграція телефонних і комп'ютерних додатків стає прозорою [17].

Іншим прикладом може служити система обробки уніфікованих повідомлень (unified messaging). Завдяки цій обробці абонент корпоративної телефонної системи може обмінюватися голосовими повідомленнями, повідомленнями електронної пошти або факсу за допомогою одного термінального пристрою, яким може служити навіть стільниковий телефон абонента. Пройшовши процедуру авторизації в системі, абонент може дізнатися вміст своєї поштової скриньки за допомогою мовного синтезатора або послати факс, використовуючи функції автоматичного розпізнавання мови.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						13
Змн.	Арк.	№ докум.	Підпис	Дата		

В даний час на ринку змагаються два підходи до побудови корпоративної телефонної системи. За IP-телефонію виступають виробники, які прийшли зі світу мереж передачі даних. А вендори, десятиліттями робили традиційні УАТС, наполягають на рішеннях, які доповнюють звичайні станції новими можливостями. По всій видимості, обидва ці підходи будуть співіснувати досить довго, але вже зараз помітна тенденція до їхнього зближення.

Перерахуємо деякі недоліки IP-телефонії.

– Незаперечною перевагою стандартної телефонної мережі до сих пір залишається можливість дзвонити навіть при відсутності електроживлення. Для телефонів VoIP потрібно не тільки електроживлення, але і широкопasmовий доступ в Інтернет.

– Передача голосу через VoIP забезпечує якість передачі з найвищим рівнем, ніж та, що надається мережами ISDN. У той же час, якість залежить від безлічі факторів, частину з яких можна контролювати (у власній локальній мережі), а іншу - ні (передача даних через Інтернет і якість послуг VoIP-провайдера).

При зв'язку VoIP використовуються послуги більшого числа компаній, ніж у випадку традиційної мережі. Наприклад, це можуть бути кілька операторів VoIP, що надають послуги місцевого й далекого телефонного зв'язку, інтернет-провайдер, що надає доступ до операторів VoIP. Чим більше учасників залучено в процес, тим складніше забезпечити узгодження дій по наскрізному забезпеченню якості обслуговування.

Основними перевагами пакетної телефонії для корпоративних користувачів є такі:

- розподілена комутація і гнучка маршрутизація викликів;
- можливість інтеграції пакетної телефонії з методами комп'ютерної обробки телефонних повідомлень, що призвело до появи так званих центрів обробки викликів (Call-center);
- ефективне використання вкладених грошових коштів за рахунок експлуатації єдиної уніфікованої телекомунікаційної мережі;

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		14

– підтримка віддалених користувачів, що дозволяє співробітникам компанії, які мають доступ в Інтернет, користуватися не тільки ресурсами корпоративної мережі даних, але і повним набором функцій офісної телефонної станції.

Важливими чинниками є відсутність дорогих і прив'язаних до виробника центральних компонентів, а також можливість поступового фінансування створення КТМ.

1.2 Компоненти IP-телефонії

Можливість передачі голосових повідомлень через мережу з пакетною комутацією вперше була реалізована в 1993 році. Дана технологія отримала назву VoIP (Voice over IP) [2], [4]. VoIP - система зв'язку, при якій аналоговий звуковий сигнал від одного абонента дискретизується (кодується) в цифровий вигляд, компресує і пересилається по цифрових каналах зв'язку до другого абонента, де проводиться зворотна операція - декомпресія, декодування і відтворення аналогового сигналу. Одним з приватних додатків даної технології є IP-телефонія - послуга з передачі телефонних розмов абонентів по протоколу IP.

Архітектура мережі VoIP може бути представлена у вигляді двох площин. Нижня відображає транспортний механізм негарантованої доставки мультимедійного трафіку у вигляді ієрархії протоколів RTP / UDP / IP, а верхня - механізм управління обслуговуванням викликів. Її ключовими протоколами є H.323 ITU-T, SIP, MGCP і MEGACO [2], що представляють собою різні реалізації обслуговування викликів в мережах IP-телефонії.

Транспортний протокол реального часу (Real-time Transport Protocol, RTP) надає транспортні послуги мультимедійним додаткам. Він не гарантує доставку і правильний порядок пакетів, але дозволяє додаткам виявити втрату або порушення порядку проходження пакетів за рахунок присвоєння кожному з них

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						15
Змн.	Арк.	№ докум.	Підпис	Дата		

номерф. Протокол призначений для роботи в режимах передачі «точка-точка» або «точка-безліч точок» і не залежить від транспортного механізму. Однак для цього зазвичай використовується протокол UDP.

RTP працює спільно з протоколом управління реального часу (Real Time Control Protocol, RTCP), що забезпечує управління потоком даних і контроль перевантаження каналу. Учасники сеансу RTP періодично обмінюються пакетами RTCP зі статистичними даними (кількість відправлених пакетів, число втрачених і т. д.), які можуть бути використані відправником мультимедіа, наприклад, для динамічної корекції швидкості передачі і навіть зміни типу навантаження.

При проектуванні КТМ на початковому етапі необхідно вибрати протокол з чотирьох згаданих, при цьому, відповідно до цих протоколів, буде використаний спосіб побудови.

Перший спосіб побудови мережі спирається на протокол H.323, короткий опис якого наведено нижче.

Другий спосіб відповідає побудові мережі на базі протоколу SIP, більш докладний опис наведений нижче.

Третій спосіб побудови мережі IP-телефонії спирається на протокол Media Gateway Control Protocol (MGCP) [2], запропонований робочою групою MEGACO комітету IETF. Архітектура цього протоколу, мабуть, найбільш проста з точки зору функціональності. Мережа MGCP містить шлюз (Media Gateway, MG), що виконує перетворення мовної інформації між мережами ТМЗК та IP-телефонії, шлюз сигналізації (Signaling Gateway, SG), забезпечує обробку сигнальної інформації, а також схожий з воротарем мережі H.323 контролер шлюзів (Call Agent), здійснює функції управління шлюзами.

Четвертий спосіб побудови мережі IP, який представляє собою удосконалення MGCP, розроблений групою MEGACO комітету IETF разом з 16 SG ITU-T, тому його називають протоколом MEGACO / H.248. Від свого старшого брата він відрізняється насамперед іншою схемою організації зв'язку. Завдяки їй контролер MEGACO / H.248 здатний змінювати топологію зв'язку

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		16

портів, що дозволяє гнучко управляти конференціями. протокол MEGACO підтримує два способи бінарного кодування [2].

1.3 Протоколи мереж IP-телефонії

1.3.1 Аналоговий протокол H.323

Серед мультимедійних стандартів найбільш досліджено стандарт H.323 ІТУ-Т, до того ж він постійно вдосконалюється і має шість версій [16]. Рекомендація H.323, історично перший спосіб здійснення викликів в мережі IP, передбачає наступні види інформаційного обміну:

- цифрове аудіо;
- цифрове відео;
- дані (обмін файлами або зображеннями);
- управління з'єднанням (обмін інформацією про підтримувані функціях, управління логічними каналами і т. д.);
- управління встановленням і роз'єднанням з'єднань та сеансів зв'язку.

Рекомендації H.323 визначають технічні вимоги для аудіо- та відеокомунікаційної служб в ЛОМ з пакетною комутацією. У загальну структуру H.323 входить і сімейство стандартів документ-конференцій T.120. У сферу впливу рекомендацій H.323 не входить ЛОМ як така, проте елементи системи ВКС, необхідні для взаємодії з мережами комутації каналів, увійшли до складу цих рекомендацій. На рисунку 1.1 представлено склад стандарту і взаємозв'язок його компонент.

Рекомендації H.323 визначає наступні елементи архітектури мережі IP-телефонії:

- термінал;
- шлюз (Gateway);

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						17
Змн.	Арк.	№ докум.	Підпис	Дата		

- контролер (Gatekeeper), іноді званий як ПЗ управління з'єднаннями або воротар;
- пристрій багатоточкового конференц-зв'язку (MCU);
- термінал H.323.

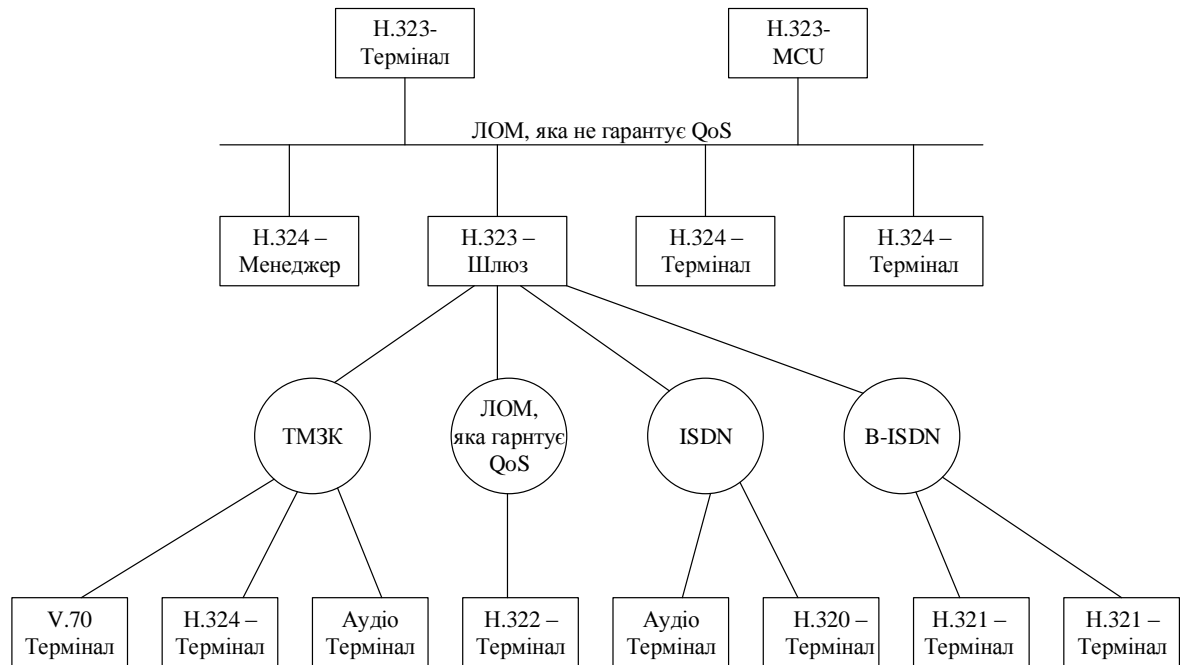


Рисунок 1.1 - Схема взаємодії H.323-системи з стандартними H.3xx-системами

Термінал. Терміналом далі називається всяке кінцеве мережеве пристрій, який забезпечує можливість двобічної комунікації в реальному часі. На рисунку 1.2 представлені можливі компоненти H.323-терміналу. Всі H.323-термінали повинні забезпечувати аудіокомунікації. Прийом / передача відеоінформації та режим документ-конференції є необов'язковими (опційними) функціями. Рекомендації H.323 визначають режими роботи, необхідні для взаємодії різних аудіо, відео та / або документ-терміналів.

Всі H.323-термінали для оцінки можливостей каналу зв'язку повинні підтримувати функції управління логічним каналом, певні рекомендації H.245. Оскільки стандарт H.245 є надзвичайно громіздким, так як описує численні можливі варіанти реалізації функцій управління, то кілька виробників

обладнання для конференц-зв'язку об'єдналися і розробили більш компактну версію цього стандарту – рекомендації H.245.1 (H.245 profile 1).

H.323-термінали повинні також обов'язково підтримувати спрощену версію протоколу Q.931, для сигналізації та виклику, містити модуль, званий RAS (Registration / Admission / Status), який забезпечує функції контролю доступу, реєстрації учасників та визначення їх поточного стану, а також мати можливість реалізації протоколу RTP / RTCP для передачі аудіо- та відеоінформації по мережах з комутацією пакетів.

Опційно термінал може підтримувати обмін відео, документ-конференції за протоколами серії T.120 і виконувати функції багатовходового моста для організації групових конференцій (MCU).



Рисунок 1.2 -Функції шлюзу між ISDN і ЛОМ-терміналами

Шлюз. Шлюз є обов'язковим елементом в H.323-системі. Цей пристрій забезпечує цілий ряд сервісів, включаючи обмін інформацією між H.323-терміналом і терміналами, які визначаються іншими ІТУ-стандартами серії H для електронних конференцій. Реалізація такої функції потребує трансляцію формату кадрів і перетворення комунікаційних процедур (наприклад, H.225.0 в H.221 і H.245 в H.242 при обміні інформацією H.323-терміналу з H.320-терміналом). Крім цього, шлюз виконує перекодування аудіо і відеопотоків, а

також забезпечує функцію встановлення і розриву з'єднання між ЛВС і мережами з комутацією каналів. Рисунок 1.2 ілюструє функції шлюзу між Н.323- і Н.320-терміналами.

У загальному випадку завданням шлюзу є взаємне відображення властивостей і характеристик кінцевого конференц-обладнання ЛОМ і терміналів мереж з комутацією каналів. Основні функції шлюзу:

- встановлення з'єднання з аналоговим терміналом в телефонній мережі загального користування;
- встановлення з'єднання з віддаленим Н.320-терміналом в мережі ISDN;
- встановлення з'єднання з віддаленим Н.324-терміналом в телефонній мережі загального користування.

Зауважимо, що шлюз не потрібен, якщо немає необхідності встановлення з'єднань ЛОМ з віддаленими терміналами в мережах з комутацією каналів, тому що Н.323-термінали мають механізм встановлення безпосередніх з'єднань. Для цього використовуються процедури протоколів Н.245 і Q.931.

З відповідними транскодерами Н.323-шлюз забезпечує взаємодію Н.333-терміналу терміналами, визначеними рекомендаціями Н.320, Н.321 (АТМ ЛОМ), Н.322 (ЛОМ з гарантованим QoS) і V.70.

Велике число можливих функцій шлюзу залишається стандартизованими. Наприклад, кількість Н.323-терміналів, які можуть одночасно встановлювати з'єднання через шлюз, кількість з'єднань з мережами комутації каналів, функції перекодування аудіо / відеопотоків, можливості підтримки багатоточкових конференцій і т.д. Всі ці характеристики можуть відрізнятися в продуктах різних виробників.

Ще один елемент мережі Н.323, проксі-сервер (посередник), працює на прикладному рівні, він визначає тип додатків і виконує потрібне з'єднання.

Площина обслуговування викликів стандарту Н.323 включає три основні протоколи (рисунок 1.3):

- протокол взаємодії кінцевого обладнання з воротарем RAS (Registration, Admission and Status);

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						20
Змн.	Арк.	№ докум.	Підпис	Дата		

- протокол управління з'єднаннями H.225;
- протокол управління логічними каналами H.245.

Для передачі сигнальних повідомлень RAS використовується протокол UDP, а для передачі сигнальних повідомлень H.225 і H.245 - протокол TCP з гарантованою доставкою інформації. UDP не забезпечує гарантованої доставки інформації, тому, якщо підтвердження не було отримано в встановлений час, повідомлення передається повторно.

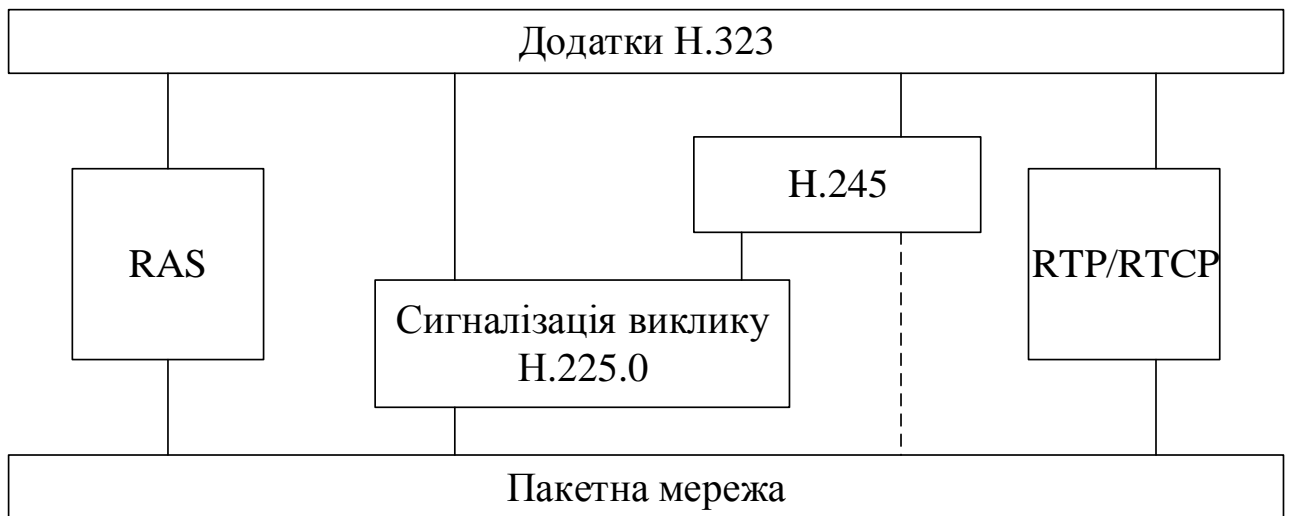


Рисунок 1.2 - Основні протоколи стеку H.323

Процес встановлення з'єднання складається з трьох етапів. На першому вирішуються завдання виявлення воротаря, реєстрації воротарем терміналів, контролю доступу терміналів до мережевих ресурсів, для чого залучається протокол RAS. На двох наступних етапах виконуються процеси сигналізації H.225 і обмін керуючими повідомленнями H.245.

Рекомендація H.225 регламентує процедури управління з'єднанням в мережах H.323 з використанням ряду сигнальних повідомлень з рекомендації Q.931 ITU-T.

Рекомендація H.245 описує процедури управління інформаційними каналами: визначення ведучого і веденого пристроїв, а також обмін даними про функціональні можливості терміналів, відкриті та закриті односпрямовані і

двонаправлені канали, що вносить затримки, режимі обробки інформації, стани інформаційних каналів шляхом організації шлейфів.

Цей обмін сигнальними повідомленнями між пристроями мережі H.323 здійснюється по логічних каналах H.245, де нульовий логічний канал, по якому передаються керуючі повідомлення, повинен бути відкритий протягом всього часу існування з'єднання [9].

Переваги, які дає стандарт МСЕ H.323 забезпечує гарантію сумісності обладнання. H.323 - гарантія якості послуг, що надаються, передачі мовної інформації з високою якістю і допустимої (керованою - у разі застосування в мережах Інтранет) затримкою, завдяки використанню швидкісних каналів передачі даних, механізмів QoS, розвиненості технології компресії мови на базі DSP [2].

1.3.2 Протокол ініціювання сеансів SIP

Протокол ініціювання сеансів - Session Initiation Protocol (SIP) є протоколом прикладного рівня і призначається для організації, модифікації і завершення сеансів зв'язку: мультимедійних конференцій, телефонних з'єднань і розподілу мультимедійної інформації. користувачі можуть брати участь в існуючих сеансах зв'язку, запрошувати інших користувачів і бути запрошеними ними до нового сеансу зв'язку.

Запрошення можуть бути адресовані певному користувачеві, групі користувачів або всім користувачам.

Протокол SIP розроблений групою MMUSIC (Multiparty Multimedia Session Control) комітету IETF (Internet Engineering Task Force), а специфікації протоколу представлені в документі RFC 2543 [18]. В основу протоколу робоча група MMUSIC заклала такі принципи.

Персональна мобільність. Користувачі можуть переміщатися без обмежень в межах мережі, тому послуги зв'язку повинні надаватися їм у будь-якому місці цієї мережі. Користувачеві присвоюється унікальний ідентифікатор, а мережа

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						22
Змн.	Арк.	№ докум.	Підпис	Дата		

надає йому послуги зв'язку незалежно від того, де він знаходиться. Для цього користувач за допомогою спеціального повідомлення -REGISTER -інформує про свої переміщення сервер визначення місця розташування.

Масштабованість мережі. Вона характеризується, в першу чергу, можливістю збільшення кількості елементів мережі при її розширенні. Серверна структура мережі, побудованої на базі протоколу SIP, в повній мірі відповідає цій вимозі.

Можливість розширення протоколу. Вона характеризується можливістю доповнення протоколу новими функціями при введенні нових послуг і його адаптації до роботи з різними додатками.

Інтеграція в стек існуючих протоколів Інтернет, розроблених IETF. Протокол SIP є частиною глобальної архітектури мультимедіа, розробленої комітетом IETF. Ця архітектура включає в себе також протокол резервування ресурсів (Resource Reservation Protocol - RSVP, RFC 2205), транспортний протокол реального часу (Real-Time Transport Protocol - RTP, RFC 1889), протокол передачі потокової інформації в реальному часі (Real-Time Streaming Protocol - RTSP, RFC 2326), протокол опису параметрів зв'язку (Session Description Protocol -SDP, RFC 2327). Однак функції протоколу SIP не залежать ні від одного з цих протоколів.

Взаємодія з іншими протоколами сигналізації. Протокол SIP може бути використаний спільно з протоколом H.323 [2]. Можливо також взаємодія протоколу SIP з системами сигналізації ТМЗК - DSS1 і ОКС7. Для спрощення такого взаємодії сигнальні повідомлення протоколу SIP можуть переносити не тільки специфічний SIP-адреса, а й телефонний номер формату E.164 або будь-якого іншого формату. Крім того, протокол SIP, нарівні з протоколами H.323 і ISUP / IP, може застосовуватися для синхронізації роботи пристроїв управління шлюзами, в цьому випадку він повинен взаємодіяти з протоколом MGCP. Іншою важливою особливістю протоколу SIP є те, що він пристосований до організації доступу користувачів мереж IP-телефонії до послуг

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		23

інтелектуальних мереж, і існує думка, що саме цей протокол стане основним при організації зв'язку між зазначеними мережами [2].

Інтеграція протоколу SIP з IP-мережами. Однією з найважливіших особливостей протоколу SIP є його незалежність від транспортних технологій. В якості транспорту можуть використовуватися протоколи X.25, Frame Relay, AAL5 / ATM, IPX і ін [6]. Структура повідомлень SIP не залежить від обраної транспортної технології. Але, водночас, перевага віддається технології маршрутизації пакетів IP і протоколу UDP. При цьому, правда, необхідно створити додаткові механізми для надійної доставки сигнальної інформації. До таких механізмів відносяться повторна передача інформації при її втраті, підтвердження прийому і ін.

Тут же слід зазначити те, що сигнальні повідомлення можуть переноситися не тільки протоколом транспортного рівня UDP, але і протоколом TCP. Протокол UDP дозволяє швидше, ніж TCP, доставляти сигнальну інформацію (навіть з урахуванням повторної передачі непідтверджених повідомлень), а також вести паралельний пошук місця розташування користувачів і передавати запрошення до участі в сеансі зв'язку в режимі під LGPL. В свою чергу, протокол TCP спрощує роботу з міжмережевими екранами (firewall), а також гарантує надійну доставку даних. При використанні протоколу TCP різні повідомлення, які стосуються кільком особам, або можуть передаватися по одному TCP-з'єднанні, або для кожного запиту і відповіді на нього може відкриватися окреме TCP-з'єднання.

По мережі з маршрутизацією пакетів IP може передаватися призначена для користувача інформація практично будь-якого виду: мова, відео та дані, а також будь-яка їх комбінація, названа мультимедійною інформацією. При організації зв'язку між терміналами користувачів необхідно сповістити зустрічну сторону, якого роду інформація може прийматися (передаватися), алгоритм її кодування і адреса, на який слід передавати інформацію. Таким чином, одним з обов'язкових умов організації зв'язку при допомоги протоколу SIP є обмін між сторонами даними про їх функціональні можливості. Для цієї мети найчастіше

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						24
Змн.	Арк.	№ докум.	Підпис	Дата		

використовується протокол опису сеансів зв'язку - SDP (Session Description Protocol). Оскільки протягом сеансу зв'язку може проводитися його модифікація, передбачена передача повідомлень SIP з новими описами сеансу засобами SDP.

Для передачі мовної інформації комітет IETF пропонує використовувати протокол RTP, але сам протокол SIP не виключає можливість застосування для цих цілей інших протоколів.

У протоколі SIP не реалізовані механізми управління потоками інформації та надання гарантованої якості обслуговування. Крім того, протокол SIP не призначений для передачі користувацької інформації, в його повідомленнях може переноситися інформація лише обмеженого обсягу. При перенесенні через мережу занадто великого повідомлення SIP не виключена його фрагментація на рівні IP, що може вплинути на якість передачі інформації.

Протокол SIP передбачає організацію конференцій трьох видів:

- в режимі під LGPL (multicasting), коли інформація передається на один multicast-адрес, а потім доставляється мережею кінцевим адресатам;
- за допомогою пристрою управління конференції (MCU), до якого учасники конференції передають інформацію в режимі точка-точка, а вона, у свою чергу, обробляє її (тобто змішує або комутує) і розсилає учасникам конференції;
- шляхом з'єднання кожного користувача з кожним в режимі точка-точка.

Протокол SIP дає можливість приєднання нових учасників до вже існуючого сеансу зв'язку, тобто двосторонній сеанс може перейти в конференцію. На закінчення дослідження інтеграції протоколу SIP з IP-мережами, слід зазначити те, що розроблені методи спільної роботи цього протоколу з перетворювачем мережевих адрес - Network Address Translator (NAT).

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		25

1.4 Постановка задачі

Необхідність вибору рішень виникає при побудові тієї чи іншої системи телефонного зв'язку. Існує ряд типових задач при введенні в експлуатацію системи телефонного зв'язку реалізованої на технології VoIP в загальному і технології побудованої на протоколі SIP зокрема, які вимагають обґрунтованого і найбільш раціонального рішення.

Для нашого випадку основна складова цих завдань представляється сполученням SIP-мережі з іншими телефонними мережами за допомогою різних шлюзів. На додаток до сказаного, однією з пріоритетних завдань було вибір рішення для телефонної мережі віддаленого офісу компанії.

Офіс компанії знаходиться за містом, де необхідно провести інтернет і КТМ, забезпечити переадресацію дзвінків на міські і мобільні телефони 46 співробітників.

В телефонному зв'язку офісу прийматимуть участь 23 програмних і 23 апаратних IP-телефони. У перспективі офіс буде розширюватися та створюватимуться філії.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		26

2 ПРОЕКТУВАННЯ МЕРЕЖІ ПЕРЕДАЧІ ГОЛОСУ

2.1 Вибір протоколу IP-телефонії

При побудові корпоративної телефонної мережі на базі IP-телефонії одним з важливих питань є вибір протоколу встановлення з'єднань. Існує три види таких протоколів і, отже, три підходи до побудови мереж IP-телефонії: H.323, що є основним стандартом для мережевих мультимедіа-додатків, SIP, протоколи, що використовують принципи декомпозиції шлюзів, наприклад MGCP (RFC 2705). Найбільш поширені протоколи на базі яких будуються КТМ, це H.323 і SIP, тому вибір буде зроблений серед цих протоколів.

Перш ніж почати порівняння функціональних можливостей протоколів SIP і H.323, нагадаємо, що протокол SIP значно молодший від свого суперника, і досвід його використання в мережах зв'язку непорівнянний з досвідом використання протоколу H.323. Існує ще один момент, на який слід звернути увагу. Інтенсивне впровадження технології передачі мовної інформації по IP-мережі потребує постійного нарощування функціональних можливостей як протоколу H.323 (до теперішнього часу затверджена вже шоста версія протоколу), так і протоколу SIP (затверджена друга версія протоколу). Цей процес призводить до того, що переваги одного з протоколів переймають іншим.

Обидва протоколи є результатом рішення одних і тих же завдань фахівцями ІТУ-Т і комітету ІETF. До рішення ІТУ можна віднести:

- переклад з'єднання в режим утримання (Call hold);
- перемикання зв'язку (Call Transfer);
- переадресація (Call Forwarding);
- повідомлення про новий виклик під час зв'язку (Call Waiting);
- конференція.

Порівняння протоколів виконується за кількома критеріями.

Додаткові послуги. Набір послуг, що надаються обома протоколами, приблизно однаковий.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						27
Змн.	Арк.	№ докум.	Підпис	Дата		

Протокол SIP передбачає три способи організації конференції: з використанням пристрою управління конференціями MCU, режиму під LGPL і з'єднань учасників один з одним. В останніх двох випадках функції управління конференціями можуть бути розподілені між терміналами, тобто центральний контролер конференцій не потрібен. Це дозволяє організовувати конференції з практично необмеженою кількістю учасників.

Рекомендація H.323 передбачає ті ж три способи, але управління конференцією у всіх випадках проводиться централізовано контролером конференцій MC (Multipoint Controller), який обробляє всі сигнальні повідомлення. Тому для організації конференції, по-перше, необхідна наявність контролера MC у одного з терміналів, по-друге, учасник з активним контролером MC не може вийти з конференції. Крім того, при великому числі учасників конференції MC може стати «вузьким місцем» [2].

Протокол SIP з самого початку орієнтований на використання в IP-мережах з підтримкою режиму під LGPL інформації. Цей механізм використовується в протоколі SIP не тільки для доставки мовної інформації (як в протоколі H.323), але і для перенесення сигнальних повідомлень. Наприклад, в режимі під LGPL може передаватися повідомлення INVITE, що полегшує визначення місця розташування користувача і є дуже зручним для центрів обслуговування викликів (Call-center) при організації групових оповіщень.

У той же час, протокол H.323 надає більше можливостей управління послугами, як в частині аутентифікації і обліку, так і в частині для контролю використання мережевих ресурсів. Можливості протоколу SIP в цій частині не такі широкі. У протоколі SIP є можливість вказувати пріоритети в обслуговуванні викликів, оскільки в багатьох країнах існують вимоги надавати переваги деяким користувачам. В протоколі H.323 такої можливості немає. Крім того, користувач SIP-мережі може реєструвати кілька своїх адрес і вказувати пріоритетність кожного з них.

Персональна мобільність користувачів. Протокол SIP має хороший набір засобів підтримки персональної мобільності користувачів, в число яких входить

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		28

переадресація виклику до нового місця розташування користувача, одночасний пошук за кількома напрямками (з виявленням зациклення маршрутів) і т.д. В протоколі SIP це організовується шляхом реєстрації на сервері визначення місця розташування, взаємодія з яким може підтримуватися будь-яким протоколом. Персональна мобільність підтримується і протоколом H.323, але менш гнучко.

Можливість розширення протоколу. Необхідною і важливою в умовах еволюціонування ринку є можливість введення нових версій протоколів і забезпечення сумісності різних версій одного протоколу. Можливість розширення (extensibility) протоколу забезпечується:

- узгодженням параметрів;
- стандартизацією кодеків;
- модульність архітектури.

Протокол SIP досить просто забезпечує сумісність різних версій. Поля, які незрозумілі обладнанню, просто ігноруються. Це зменшує складність протоколу, а також полегшує обробку повідомлень та впровадження нових послуг. клієнт може запросити будь-яку послугу за допомогою заголовка Require. Сервер, отримавши запит з таким заголовком, перевіряє, чи підтримує він цю послугу, і якщо не підтримує, то повідомляє про це у своїй відповіді, що містить список підтримуваних послуг.

У разі необхідності, в організації IANA (Internet Assigned Numbers Authority) можуть бути зареєстровані нові заголовки. Для реєстрації в IANA відправляється запит з ім'ям заголовка і його призначенням. Назва заголовка вибирається таким чином, щоб вона говорила про його призначення. Зазначеним чином розробник може впроваджувати нові послуги.

Для забезпечення сумісності версій протоколу SIP визначено шість основних видів запитів і 6 класів відповідей на запити. Так як визначальною в кодах відповідей є перша цифра, то обладнання може вказувати та інтерпретувати тільки її, а інші цифри коду тільки доповнюють зміст і їх аналіз не є обов'язковим.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		29

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

Нові функціональні можливості вводяться в протокол H.323 з допомогою поля NonStandardParameter [2]. Воно містить код виробника і, слідом за ним, код послуги, який дійсний тільки для цього виробника. Це дозволяє виробникові розширювати послуги, проте є певні обмеження. По-перше, неможливо вимагати від сторони, яка викликається, інформацію про підтримувані нею послуги, по-друге, неможливо додати нове значення вже існуючого параметра. Існують також проблеми, пов'язані із забезпеченням взаємодії обладнання різних виробників.

На розширення можливостей протоколу, як і на сумісність обладнання, що його реалізує, впливає і набір кодеків, підтримуваних протоколом. У протоколі SIP для передачі інформації про функціональні можливості терміналу використовується протокол SDP. Якщо виробник підтримує якийсь особливий алгоритм кодування, то цей алгоритм просто реєструється в організації IANA. У протоколі H.323 всі кодекси повинні бути стандартизовані. Тому додатки з нестандартними алгоритмами кодування можуть зіткнутися з проблемами при реалізації їх на базі протоколу H.323.

Протокол SIP складається з набору закінчених компонентів (Модулів), які можуть замінюватися в залежності від вимог і можуть працювати незалежно один від одного. Цей набір включає в себе модулі підтримки сигналізації для базового з'єднання, для реєстрації і для визначення місця розташування користувача, які не залежать від модулів підтримки якості обслуговування (QoS), роботи з директоріями, опису сеансів зв'язку, розгортанням послуг (service discovery) і управлінням конфігурацією.

Архітектура протоколу H.323 монолітна і являє собою інтегрований набір протоколів для одного застосування. Протокол складається з трьох основних складових, і для створення нової послуги може знадобитися модифікація кожної з них.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						30
Змн.	Арк.	№ докум.	Підпис	Дата		

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

Необхідно також мати на увазі зонову архітектуру мережі H.323, що дозволяє забезпечити розширюваність мережі шляхом збільшення кількості зон [2].

Час встановлення з'єднання. Наступною істотною характеристикою протоколів є час, який потрібен, щоб встановити з'єднання. У запиті INVITE протоколу SIP міститься вся необхідна для встановлення з'єднання інформація, включаючи опис функціональних можливостей терміналу. Таким чином, в протоколі SIP для встановлення з'єднання потрібна одна транзакція, а в протоколі H.323 необхідно проводити обмін повідомленнями декілька разів. З цих причин витрати часу на встановлення з'єднання в протоколі SIP значно менші, ніж витрати часу в протоколі H.323. Проте, при використанні інкапсуляції повідомлень H.245 в повідомлення H.225 або процедури Fast Connect час встановлення з'єднання значно зменшується.

Крім того, на час встановлення з'єднання впливає також і нижній транспортний протокол, який переносить сигнальну інформацію. Ранні версії протоколу H.323 передбачали використання для перенесення сигнальних повідомлень H.225 і H.245 тільки протоколу TCP, і лише третя версія протоколу передбачає можливість використання протоколу UDP. Протоколом SIP використання протоколів TCP і UDP передбачалося з самого початку.

Оцінка часу встановлення з'єднання виробляється в умовних одиницях - RTT (round trip time) - і становить для протоколу SIP $1,5 + 2,5$ RTT, а для протоколу H.323 $6-7$ RTT [2].

Адресація. До числа системних характеристик відноситься і передбачена протоколами адресація. Використання URL є сильною стороною протоколу SIP та дозволяє легко інтегрувати його в існуючу систему DNS-серверів і

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						31
Змн.	Арк.	№ докум.	Підпис	Дата		

впроваджувати в обладнання, що працює в IP-мережах. Користувач отримує можливість переправляти виклики на Web-сторінки або використовувати електронну пошту. Адресою в SIP може також служити телефонний номер з адресою використовуваного шлюзу.

У протоколі H.323 використовуються транспортні адреси і alias-адреси. В якості останнього може використовуватися телефонний номер, ім'я користувача або адреса електронної пошти. Для перетворення alias-адреси в транспортну адресу обов'язкова участь вогоратаря.

Складність протоколу. Протокол H.323, безсумнівно, є складнішим, ніж протокол SIP. Загальний обсяг специфікацій протоколу H.323 становить приблизно 700 сторінок. Обсяг специфікацій протоколу SIP становить 150 сторінок. Протокол H.323 використовує велику кількість інформаційних полів в повідомленнях (до 100), при декількох десятках таких же полів в протоколі SIP. При цьому для організації базового з'єднання в протоколі SIP досить використовувати всього три типи запитів (INVITE, BYE і ACK) і кілька полів (To, From, CallID, CSeq).

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

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

Досить складним є взаємодія протоколу H.323 з фаєрволом (firewall). Крім того, в протоколі H.323 існує дублювання функцій. Так, наприклад, обидва

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						32
Змн.	Арк.	№ докум.	Підпис	Дата		

протоколи H.245 і RTCP мають засоби управління конференцією і здійснення зворотнього зв'язку.

На основі проведеного вище порівняння можна зробити висновок про те, що протокол SIP більше підходить для використання в КТМ, де інтегровані різні види сервісів. Більш вигідна, з точки зору побудови, архітектура мережі і простота реалізації додаткового функціоналу роблять його ще більш привабливим для впровадження.

Необхідно відзначити ще один факт на користь вибору SIP, це те що ключові архітектурні елементи мережі, є практично безкоштовними з відкритим вихідним кодом (Open Source), що є більш вигідним рішенням, з економічної точки зору.

2.2 Архітектура мережі SIP

У певному сенсі прабатьком протоколу SIP є протокол перенесення гіпертексту - HTTP (Hypertext Transfer Protocol, RFC 2068). Протокол SIP успадкував від нього синтаксис і архітектуру «Клієнт-сервер», яку ілюструє рисунок 2.1.

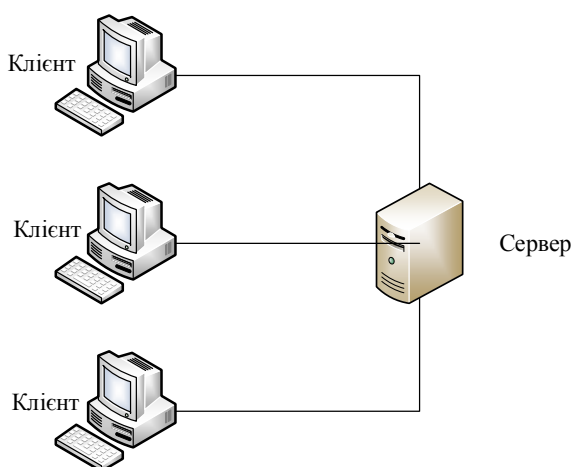


Рисунок 2.1 – Архітектура «Клієнт - сервер»

Клієнт видає запити, в яких вказує, що він бажає отримати від сервера. Сервер приймає запит, обробляє його і видає відповідь, яка може містити повідомлення про успішне виконання запиту, повідомлення про помилку або інформацію, затребувану клієнтом.

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

Термінал. У разі, коли клієнт і сервер взаємодіють безпосередньо з користувачем (тобто реалізовані в крайовому обладнанні користувача), вони називаються, відповідно, клієнтом агента користувача - User Agent Client (UAC) - і сервером агента користувача - User Agent Server (UAS). Потрібно відзначити, що сервер UAS і клієнт UAC можуть (але не зобов'язані) безпосередньо взаємодіяти з користувачем, а інші клієнти і сервери SIP цього робити не можуть. Якщо в пристрої присутні і сервер UAS, і клієнт UAC, то вони називається агентом користувача - User Agent (UA), а за своєю суттю є термінальним обладнання SIP.

Крім терміналів визначені два основних типи мережевих елементів SIP: проксі-сервер (proxy server) і сервер переадресації (Redirect server).

Проксі-сервер (від англійського proxy - представник) представляє інтереси користувача в мережі. Він приймає запити, обробляє їх і, в залежності від типу запиту, виконує певні дії. Це може бути пошук і виклик користувача, маршрутизація запиту, надання послуг і т.д. Проксі-сервер складається з клієнтської і серверної частин, тому може приймати виклики, ініціювати власні запити і повертати відповіді.

Проксі - сервер може бути фізично суміщений з сервером позиціонування (в цьому випадку він називається registrar) або існувати окремо від цього сервера, але мати можливість взаємодіяти з ним по протоколам LDAP (RFC 1777), rwhois (RFC 2167) і по будь-яким іншим протоколам.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		34

Передбачено два типи проксі-серверів - зі збереженням станів (stateful) і без збереження станів (stateless).

Сервер першого типу зберігає в пам'яті вхідний запит, який став причиною генерації одного або декількох вихідних запитів. Ці вихідні запити сервер також запам'ятовує.

Сервер без збереження станів просто ретранслює запити і відповіді, які отримує. Він працює швидше, ніж сервер першого типу, так як ресурс процесора не витрачається на запам'ятовування станів, внаслідок чого сервер цього типу може обслужити більшу кількість користувачів. Недоліком такого сервера є те, що на його базі можна реалізувати лише найбільш прості послуги.

Алгоритм роботи користувачів з проксі-сервером виглядає наступним чином. Постачальник послуг IP-телефонії повідомляє адрес проксі-сервера своїм користувачам. Викликаючий користувач передає до проксі-сервера запит з'єднання. Сервер обробляє запит, визначає місце розташування викликається користувача і передає запит цьому користувачеві, а потім отримує від нього відповідь, підтверджує успішну обробку запиту, і транслює цю відповідь користувачеві, який передала запит. Проксі-сервер може модифікувати деякі заголовки повідомлень, які він транслює, причому кожен сервер, який обробив запит в процесі його передачі від джерела до приймача, повинен вказати це в SIP-запиті для того, щоб відповідь на запит повернувся тим самим шляхом.

Сервер переадресації призначений для визначення поточного адреси викликається користувача. Викликаючий користувач передає до сервера повідомлення з відомим йому адресою користувача, який викликається, а сервер забезпечує переадресацію виклику на поточну адресу цього користувача. Для реалізації цієї функції з сервер переадресації повинен взаємодіяти з сервером визначення місця розташування.

Сервер переадресації не термінує виклики як сервер RAS і не ініціює власні запити як проксі-сервер. Він тільки повідомляє адресу або викликає користувача, або проксі-сервера. За цією адресою ініціатор запиту передає новий

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		35

запит. Сервер переадресації не містить клієнтську частину програмного забезпечення.

Але користувачеві не обов'язково зв'язуватися з будь-яким SIP-сервером. Він може сам викликати іншого користувача за умови, що знає його поточний адресу.

Протоколом SIP передбачені 3 основні сценарії встановлення з'єднання: за участю проксі-сервера, за участю сервера переадресації і безпосередньо між користувачами. Різниця між перерахованими сценаріями полягає в тому, що по-різному здійснюється пошук і запрошення користувача, який викликається. У першому випадку ці функції покладає на себе проксі-сервер, а викликаючому користувачеві необхідно знати тільки постійний SIP-адрес користувача, який викликається. У другому випадку що викликає сторона самостійно встановлює з'єднання, а сервер переадресації лише реалізує перетворення постійного адреси абонента в його поточну адресу. І, нарешті, в третьому випадку викликаючому користувачеві для встановлення з'єднання необхідно знати поточну адресу користувача, який викликається.

Встановлення з'єднання з участю проксі-сервера. Адміністратор мережі повідомляє адресу цього проксі-сервера користувачам. Викликаючий користувач передає запит INVITE (1) на адресу проксі-сервера і порт 5060. У запиті користувач вказує відому йому адресу користувача, який викликається. Проксі-сервер запитує поточну адресу користувача, що викликається у сервера позиціонування (2), який і повідомляє йому цю адресу (3). Далі проксі-сервер передає запит INVITE безпосередньо обладнанню, що викликається (4). Знову в запиті містяться дані про функціональні можливості викликаючого терміналу, але при цьому в запит додається поле Via з адресою проксі-сервера для того, щоб відповіді на зворотному шляху йшли через нього. Після прийому і обробки запиту обладнання, що викликається, повідомляє своєму користувачеві про вхідний дзвінок, а зустрічній стороні передає відповідь 180 Ringing (5), копіюючи в нього із запиту поля To, From, Call-ID, CSeq і Via. Після прийому виклику користувачем зустрічній стороні передається повідомлення 200 OK (6),

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						36
Змн.	Арк.	№ докум.	Підпис	Дата		

що містить дані про функціональні можливості терміналу, що викликається, у форматі протоколу SDP. Термінал викликаючого користувача підтверджує прийом відповіді запитом АСК (7). На цьому фаза встановлення з'єднання закінчена і починається розмовна фаза.

По завершенні розмовної фази однієї зі сторін передається запит BYE (8), який підтверджується відповіддю 200 ОК (9).

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

Сценарій встановлення з'єднання через проксі-сервер представлено на ДП.КСМ.111862/16.00.00.000 С1.

2.3 Методи забезпечення якості обслуговування

Існує два методи забезпечення якості обслуговування: IntServ і DiffServ. Хотілося б більш детально розглянути ключові аспекти даних методів, так як якість обслуговування реалізовано саме за допомогою диференціального методу.

2.4.1 Архітектура інтегрованих послуг IntServ

Integrated Service (IntServ, RFC +1633) - модель інтегрованого обслуговування [10]. Може забезпечити наскрізну (End-to-End) якість обслуговування, гарантуючи необхідну пропускну здатність.

IntServ використовує для своїх цілей протокол сигналізації RSVP, дозволяє додаткам ставити наскрізні вимоги до ресурсів і містить механізми забезпечення даних вимог. IntServ можна коротко охарактеризувати як резервування ресурсів (Resource reservation).

Протокол RSVP. Даний протокол дозволяє додаткам посилати сигнали в мережу про свої QoS-вимоги для кожного потоку. Щоб визначити кількісні

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						37
Змн.	Арк.	№ докум.	Підпис	Дата		

характеристики цих вимог з метою управління доступом, використовуються службові параметри.

Протокол RSVP сигналізує про запити резервування ресурсів по доступному маршрутизованому шляху в мережі. При цьому RSVP не виробляє власну маршрутизацію; навпаки, цей протокол був розроблений для використання інших, більш потужних протоколів маршрутизації. Як і будь-який інший IP-трафік, при визначенні шляху для даних і керуючого трафіку RSVP покладається на застосовуваний в мережі протокол маршрутизації.

Робота протоколу RSVP. Кінцеві системи використовують протокол RSVP, щоб пристрій запитував у мережі певного рівня QoS від імені потоку даних програми. RSVP-запити передаються по мережі при проходженні кожного вузла, який застосовується для передачі потоку. Протокол RSVP намагається зарезервувати ресурси для потоку даних на кожному з цих вузлів.

RSVP-резервування ресурсів для потоку можна розбити на два типи: індивідуальне і загальне.

Індивідуальне резервування (distinct reservations) застосовується в тих додатках, в яких кілька джерел даних можуть відправляти інформацію одночасно. В відеододатках кожен відправник генерує індивідуальний потік даних, для якого необхідно здійснювати окреме управління доступом і планування черги на всьому шляху до одержувача. Отже, для такого потоку необхідно здійснювати окреме резервування ресурсів для кожного відправника і для кожного каналу в дорозі.

Найпростіший випадок індивідуального резервування ресурсів спостерігається на прикладі додатка з одноадресним трафіком, де є тільки один відправник і один одержувач.

Загальна резервування (shared reservations) застосовується в тих додатках, в яких кілька джерел даних не схильне передавати інформацію одночасно, наприклад цифрові аудіододатки, такі як додатки VoIP. В цьому випадку, оскільки в будь-який окремо взятий проміжок часу розмова веде невелике число людей, інформація передається лише невеликою обмеженою кількістю

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						38
Змн.	Арк.	№ докум.	Підпис	Дата		

відправників. Такий потік не потребує окремого резервування ресурсів для кожного відправника, для нього потрібно всього лише одне резервування, яке при необхідності можна буде застосувати до будь-якого відправника в групі.

Типи послуг. Протокол RSVP надає два типи інтегрованих послуг, які одержувачі можуть запитувати за допомогою повідомлень RSVP: службу регульованою навантаження і службу гарантованої бітової швидкості.

Служба регульованою навантаження (controlled load service) забезпечує гарантію того, що зарезервованій потік досягне свого пункту призначення з мінімальним втручанням з боку трафіку, що доставляється без гарантій. Більш того, в реалізації цієї послуги компанією Cisco передбачена ізоляція окремих зарезервованих потоків. Ізоляція потоку дозволяє виключити вплив інших присутніх в мережі зарезервованих потоків при резервування ресурсів.

Як правило, служба регульованою навантаження застосовується при передачі трафіку Internet-додатків, чутливих до перевантажень в мережі.

Служба гарантованої бітової швидкості (guaranteed bit rate service) забезпечує обмеження затримки без відкидання дейтаграм, задовольняючих параметрам трафіку, в умовах відсутності збоїв в роботі мережевих компонентів або змін в інформації про маршрутах під час життя потоку. Ця служба гарантує мінімальне втручання з боку трафіку, доставляється без гарантій, ізоляцію зарезервованих потоків і числове вираз максимальної затримки.

Служба гарантованої бітової швидкості може забезпечити тільки максимальну, але не мінімальну або середню затримку дейтаграм. Служба гарантованої бітової швидкості найкраще підходить для тих додатків масштабу реального часу, які дозволяють відтворювати аудіо- та відеофайли.

Масштабованість протоколу RSVP. Недоліком протоколу RSVP є те, що обсяг необхідної інформації про стан потоків збільшується з ростом числа резервування ресурсів для потоків трафіку.

Так як в Internet-магістралі в будь-який час можуть існувати багато сотні тисяч одноадресних і багатоадресних потоків, використання інформації про стан кожного потоку вважається невідповідним рішенням для магістралей Internet.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						39
Змн.	Арк.	№ докум.	Підпис	Дата		

Крім того, навіть в корпоративній мережі перешкодою для використання протоколу RSVP може бути вимога його підтримки всіма маршрутизаторами на шляху потоку.

2.4.2 Архітектура диференційованих послуг DiffServ

Архітектурну модель DiffServ можна порівняти з мостом, який з'єднує механізм гарантованої якості обслуговування моделі intserv з механізмом негарантованої доставки трафіку. Модель DiffServ забезпечує диференціювання трафіку шляхом його розбивки на класи з різних пріоритетом.

Головним завданням підходу DiffServ є визначення стандартизованого байта диференційованої послуги (DS) – байта типу обслуговування (Type of Service - ToS) з заголовком пакета IPv4 і байта класу трафіку (Traffic Class) пакета IPv6. Від даного маркування залежить прийняття рішення про просування пакета даних на кожному переході (per-hop behavior - PHB), тобто в кожному проміжному вузлі.

Архітектура диференційованих послуг забезпечує базову основу, яка може бути використана операторами для надання своїм клієнтам великого діапазону різних пропозицій в залежності від пропонованих вимог до якості обслуговування. Клієнт може вибрати необхідний рівень послуг шляхом установки відповідного значення поля коду диференційованої послуги (Differentiated Services Code Point - DSCP) для пакетів певної програми. Код диференційованої послуги визначає ланцюжок рішень про просування пакета в кожному проміжному вузлі мережі оператора або корпоративної мережі (PHB-політика).

На рисунку 2.2 представлено архітектуру диференційованих послуг DiffServ.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		40

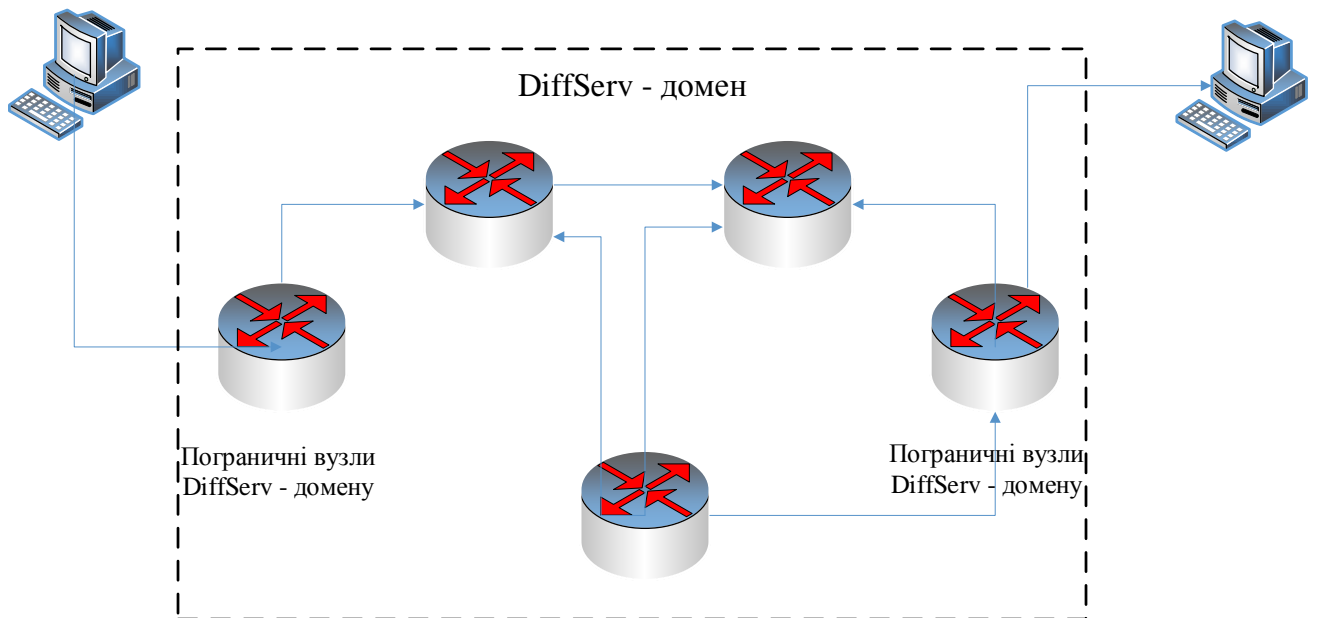


Рисунок 2.2 - Архітектура DiffServ

Архітектура методу DiffServ. РНВ-політика - політика покрокового обслуговування, визначає поведінку мережевого вузла щодо пакетів з певним значенням поля DSCP. Всі пакети потоку трафіку зі специфічною вимогою до обслуговування несуть в собі одне і те ж значення поля DSCP.

Всі вузли усередині DiffServ-домену визначають РНВ-політику, яка повинна бути застосована до пакету на основі зберігання в ньому значення поля коду диференційованої послуги. Крім того, прикордонні вузли DiffServ-домену виконують важливу функцію формування що надходить в DiffServ-домен трафіку. Формування трафіку включає в себе виконання таких функцій, як:

- класифікація пакетів (установка значення поля DSCP);
- обмеження трафіку.

Формувачі трафіку. Формувачі трафіку - це різні функції якості обслуговування, які повинні бути реалізовані в пограничних пристроях мережі. Граничні функції класифікують або маркують трафік шляхом установки відповідного значення поля DSCP, а також проводять моніторинг вхідного до мережі трафіку з метою перевірки його відповідності встановленим профілем.

Код диференційованої послуги являє собою поле, на підставі значення якого визначається спосіб обробки пакета в DiffServ-доміні. Як й функції

опрацювання трафіку може виступати функція класифікації пакетів, функція маркування DSCP-поля або ж функція дозування трафіку, наділена або повноваженнями вирівнювання трафіку, або повноваженнями відкидання пакетів.

Класифікатор пакетів вибирає пакет з потоку трафіку на підставі аналізу частини вмісту заголовка пакета. Найбільш поширений спосіб класифікації пакетів полягає в аналізі поля DSCP, однак теоретично можлива класифікація пакету на підставі значення інших полів його заголовка. Функція класифікації пакета визначає відповідний цьому пакету клас трафіку.

Функція маркування призначена для запису / перезапису поля DSCP в залежності від класу трафіку, до якого відноситься даний пакет.

Функція дозування перевіряє трафік на відповідність заданим профілем на підставі дескриптора трафіку, такого як корзина маркерів. Результати перевірки можуть передаватися функції маркування трафіку, а також як і функції вирівнювання трафіку, або функції відкидання пакетів - для прийняття відповідного рішення щодо "планових" і "позапланових" пакетів.

Функція вирівнювання трафіку (traffic shaping) здійснює затримку пакетів шляхом їх буферизації з метою задоволення параметрів заданого профілю.

Функція відкидання пакетів здійснює відкидання всіх пакетів, які задовольняють параметрам заданого профілю трафіку. Ця дія часто називають також обмеженням трафіку (traffic policing).

РНВ-політика. Мережеві вузли з підтримкою диференційованого обслуговування використовують поле DSCP в заголовку IP-пакета для визначення відповідної цьому пакету РНВ-політики. РНВ-політика може бути визначена в термінах пріоритету в наданні ресурсів по відношенню до інших РНВ-політик або ж за допомогою таких вимірюваних характеристик трафіку, як затримка пакетів, рівень втрати пакетів або тремтіння трафіку.

Як стандартна РНВ-політики в DiffServ-мережі можна розглядати негарантовану доставку трафіку. Відповідно до архітектури диференційованого обслуговування кожній РНВ-політиці рекомендується призначити певний код

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						42
Змн.	Арк.	№ докум.	Підпис	Дата		

DSCP, проте постачальник послуг може вибрати відмінні від рекомендованих значення поля DSCP для своєї власної мережі. Рекомендоване значення поля DSCP для політики негарантованої доставки пакетів дорівнює 000 000.

Існують дві стандартні PNB-політики - PNB-політика негайної передачі (EF PNB) і PNB-політика гарантованої доставки (AF PNB).

PNB-політика негайної передачі пакетів (Expedited Forwarding PNB - EF PNB). Використовується для забезпечення наскрізного обслуговування пакетів в вузлах DiffServ-домену, характерними рисами якого є низький рівень втрати пакетів, мала затримка, незначне тремтіння трафіку, а також гарантована смуга пропускання. Політика EF PNB застосовується для обслуговування трафіку таких додатків, як передача голосу по мережах IP (Voice over IP - VoIP), додатків відеоконференцій, а також для забезпечення таких послуг, як передача інформації по віртуальним орендованих каналах, оскільки ця послуга являє собою двоточкове з'єднання кінцевих вузлів DiffServ-домену. Подібний тип обслуговування досить часто називають також послугами високого класу (premium service).

Один із способів уникнути затримки пакетів, пов'язаної з виникненням великих черг є обмеження максимальної інтенсивності вхідного потоку трафіку мінімальної інтенсивністю його вихідного потоку. PNB-політика негайної передачі пакетів передбачає установку значення інтенсивності вихідного потоку трафіку, в той час як інтенсивність вхідного потоку контролюється формувачами трафіку, реалізованими в пограничних пристроях мережі. Як правило, інтенсивність вхідного і вихідного потоків вимірюється з інтервалами, рівними часу, який потрібен для передачі MTU-пакета (пакета максимального розміру, який може бути переданий через інтерфейс маршрутизатора) по даній лінії зв'язку. Коли мова йде про передачу трафіку через перевантажений сегмент мережі (а це передбачає наявність великих накопичених черг), дана функціональна можливість може бути реалізована за рахунок застосування різних механізмів обслуговування черг.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						43
Змн.	Арк.	№ докум.	Підпис	Дата		

РНВ-політика гарантованої доставки пакетів (AF РНВ). РНВ-політика гарантованої доставки пакетів (Assured Forwarding РНВ - AF РНВ) являє собою засіб, за допомогою якого постачальник послуг може забезпечити кілька різних рівнів надійності доставки ІР-пакетів, отриманих з DiffServ-домену клієнта. Політика AF РНВ є прийнятною для більшості TCP-додатків.

РНВ-політика гарантованої доставки пакетів забезпечує наявність різних рівнів обслуговування для кожного з чотирьох класів AF-трафіку. Кожному класу AF-трафіку відповідає власна чергу пакетів, що дозволяє проводити ефективне управління смугою пропускання. Кожен клас AF-трафіку характеризується трьома рівнями пріоритету відкидання пакетів (низький, середній і високий), що дозволяє реалізувати механізм управління чергою по типу механізму довільного раннього виявлення (Random Early Detection - RED).

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						44
Змн.	Арк.	№ докум.	Підпис	Дата		

3 РЕАЛІЗАЦІЯ КОРПОРАТИВНОЇ ТЕЛЕФОННОЇ МЕРЕЖІ

3.1 Рішення для телефонної мережі філії

Інтеграція телефонної мережі віддаленого філії в корпоративну телефонну мережу - одна з типових задач, витончено вирішуються за допомогою технології ІР-телефонії.

Підключення шлюзу внутрішньої мережі до міні-АТС має певні недоліки, головна з яких - неможливість організації єдиного плану нумерації у внутрішній мережі. Для здійснення викликів між корпусом А та адміністративним відділом доводилося проводити набір номера в дві стадії. Ще більше складними були правила набору корпусу А в ТМЗК.

У зв'язку з цим було прийнято рішення про модернізацію мережі ІР-телефонії філії.

Наведемо опис остаточного варіанту, який відпрацьовувався режимі моделювання. Модернізація мережі включає чотири елементи:

- перехід з протоколу Н.323 на SIP;
- заміна обладнання;
- зміна схеми включення шлюзу внутрішньої мережі та перехід на статичну маршрутизацію викликів у внутрішній мережі;
- організація зв'язку з корпоративною мережею.

Перехід на статичну маршрутизацію телефонних з'єднань був визнаний доцільним для підвищення відмовостійкості телефонної мережі. Хоча стабільність роботи використовуваного досі гейткіпера Н.323 (AquaGatekeeper) не викликала нарікань, все ж надійність цього елемента пов'язана з апаратною надійністю комп'ютера, який, до того ж, використовується для декількох додатків. У той же час, при малій кількості абонентів VoIP-мережі конфігурація статичних маршрутів на шлюзах не викликає особливих труднощів.

Для забезпечення зв'язку з корпусом А із використанням єдиного плану нумерації внутрішньої мережі було вирішено використовувати техніку «Виносу»

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						45
Змн.	Арк.	№ докум.	Підпис	Дата		

внутрішніх ліній міні-АТС за допомогою зв'язки шлюзів FXO-FXS. В якості шлюзу внутрішньої мережі буде використаний AP1100C - шлюз з 8 FXO-портами, підключеними до внутрішніх ліній міні-АТС. Кожен з портів шлюзу налаштований в режимі «гарячої лінії».

```
voice-port 0/1  
connection plar 201  
ring detect-timeout 70
```

При надходженні виклику на порт FXO 0/1 з боку міні-АТС шлюз набирає 301 (номер, присвоєний порту міні-АТС) і зіставляє набір з Dial-Peer-ами. Конфігурація Dial-Peer показана нижче.

```
dial-peer voice 201 voip  
destination-pattern 201  
session target 10.2.192.131  
session protocol sip  
codec g711alaw  
dtmf-relay rtp-2833
```

Тут 10.2.192.131 - IP-адреса відповідного FXS-шлюзу. Виклики з FXS-шлюзів в сторону міні-АТС маршрутизуються по індивідуальним префіксам, підставленим правилами перетворення номерів на FXS-шлюзах, таким чином, що кожен абонент займає свою лінію міні-АТС.

```
dial-peer voice 21 pots  
destination-pattern 21.T  
port 0/1  
forward-digits from 2  
...
```

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		46

На FXS-шлюзі кожному до порту прив'язується відповідне правило перетворення номерів.

```
! FXS
voice-port 0/1
...
translate-incoming called-number 201
...
translation-rule 201
rule 1 1T 21%99
rule 8 8T 218%99
rule 9 9 219
...
dial-peer voice 201 pots
destination-pattern 201
port 0/1
...
dial-peer voice 21 voip
destination-pattern 21.T
session target 10.2.192.129
session protocol sip
codec g711alaw
dtmf-relay rtp-2833
...
```

У міні-АТС використовує тризначний план нумерації з провідними цифрами 1 - для абонентів, безпосередньо підключених до АТС, 2 - для абонентів, підключених до АТС через VoIP-шлюзи. Правило трансляції номерів перетворює номери, відправляються на міні-АТС (1 ... - абоненти, 9 ... - ТМЗК, 8

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						47
Змн.	Арк.	№ докум.	Підпис	Дата		

... – КТМ Головного офісу) і не змінює номери IP-абонентів, що починаються з 2. При дзвінку в ТМЗК після набору «9» відбувається спроба заняття однією з відповідних ліній. Якщо вільної СО-лінії немає, абонент відразу після набору «9» чує сигнал відмови в обслуговуванні (reorder tone). Набір «8» використовується для виходу в корпоративну мережу Головного офісу з маршрутизацією по ARS.

Організація зв'язку з корпоративною телефонною мережею з мережею головного офісу, принесе значну економію затрат на послуги зв'язку, яку планується використовувати для оплати Інтернет. Схема корпоративної телефонної мережі представлена на ДП.КСМ.111862/16.00.00.001 С1.

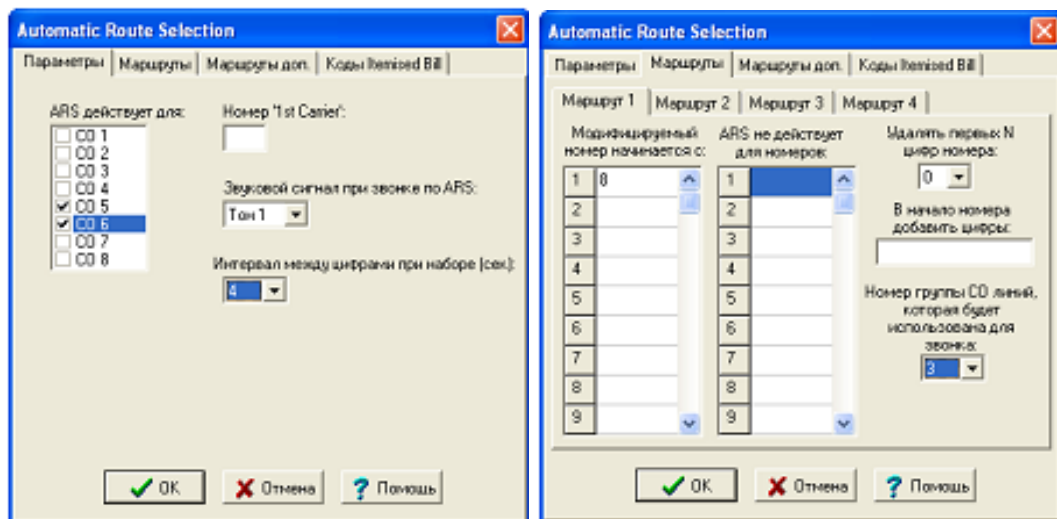


Рисунок 3.1 - Приклад конфігурації міні-АТС

Інтеграція мереж виконується за допомогою шлюзу IP-телефонії, підключеного до вільних СО-ліній міні-АТС. При цьому з'єднання при дзвінку з мережі корпусу А на будь-який номер мережі фірми буде виконуватися в одну стадію - по внутрішньому номером КТМ Головного офісу. Це досягається перетворенням номера перед його відправкою в міні-АТС. Набір номера мережі Головного офісу з міні-АТС проводиться з префіксом «8» і маршрутизується механізмом ARS. Приклад конфігурації міні-АТС зображений на рисунку 3.1.

3.2 Сполучення VoIP-мережі з ТМЗК

Для сполучення VoIP-мережі з ТМЗК необхідно використовувати медіашлюзи. Існує два підходи до реалізації такого рішення.

Підхід призначений для клієнтів, у яких в рамках корпоративної IP-телефонії вже встановлена IP-УАТС, керуюча IP-телефонами, ПК-телефонами (PC Soft phones) і / або IP-функціями, вбудованими в УАТС на базі TDM. Рішення для пакетної телефонії емулює функції традиційної УАТС (тобто авторизацію користувачів, локальну комутацію та ін.) і крім цього надає доступ до мультимедійних послуг, наприклад, онлайн-відеоконференціям. Замість установки у клієнта шлюзу IP-TDM для передачі викликів в мережу ТМЗК оператор забезпечує стандартний інтерфейс VoIP, такий як SIP або H.323. Замовник в цьому випадку підключається до операторської мережі безпосередньо через маршрутизатор доступу, який, при необхідності, використовується і для передачі даних, створюючи єдиний для голосу і даних канал передачі від клієнта до мережі оператора. вузли керування викликами (MGC, SIP Proxy або H.323 Gatekeeper), встановлені у оператора, виконують функції маршрутизації викликів, генерування записів CDR і т.д.

На ділянці сполучення телефонної мережі використовується стандарт H.323, так як він більш пристосований для взаємодії з мережами ISDN. Тому виникає необхідність в конвертації сигналізації протоколу SIP в сигналізацію протоколу H.323 і назад. Для цих цілей використовується шлюз IP-IP реалізований на платформі Cisco.

Конвертори (шлюзи) допомагають з'єднати між собою дві, а то кілька незалежних мереж. У ролі такого конвертера може виступати ПО, яке працює на платформі ПК, наприклад MERA MVTS з модулем SIP-НІТ або маршрутизатора Cisco (Cisco Multiservice IP-to-IP Gateway).

Аналоговий шлюз відповідає за наступну функціональність:

– обробка медіа-потоків і цілісність мовного тракту;

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						49
Змн.	Арк.	№ докум.	Підпис	Дата		

- передача DTMF-сигналів;
- трансляція факсових повідомлень або їх прозорий пропуск (Passthrough);
- трансляція номерів і обробка викликів;
- фільтрація напрямків і кодеків;
- розпізнавання та обробка ідентифікатора мережі оператора;
- термінування і реініціювання сигналізації і мовного тракту.

Шлюзом підтримуються наступні типи з'єднань:

- H.323 <-> H.323;
- SIP <-> H.323;
- SIP <-> SIP.

У корпоративної мережі шлюз IP-IP працює на прикордонному маршрутизатор Cisco 2851. У процесі налагодження були отримані різні результати при роботі з трьома іншими відділами організацій:

- повна сумісність;
- одностороннє проходження викликів;
- повна неможливість здійснення викликів.

У зв'язку з цим, до завершення налагодження взаємодії з іншими мережами сполучення SIP-H.323 виконано через зв'язку двох шлюзів SIPTDM-H.323.

3.3 Налаштування Asterisk-сервера на ОС Linux

Asterisk - це програмна АТС, що працює на операційних системах Linux, FreeBSD, OpenBSD, Solarix та дозволяє розгортати сучасний телефонний зв'язок на базі комп'ютерної мережі. Це дуже потужний і гнучкий продукт для бізнесу, що забезпечує новітні корпоративні телефонні сервіси. В поєднанні з необхідним інтерфейсним обладнанням, Asterisk забезпечує підключення комп'ютера до існуючих телефонних мереж та може працювати як з аналоговими лініями (FXO / FXS модулі), так і цифровими (ISDN, BRI і PRI - потоки T1/E1). За

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						50
Змн.	Арк.	№ докум.	Підпис	Дата		

допомогою певних комп'ютерних плат Asterisk можна підключити до високопропускних ліній (T1/E1), які дозволяють працювати паралельно з десятками телефонних з'єднань.

Asterisk у поєднанні з необхідним обладнанням має всі можливості класичної АТС, підтримує багато VoIP-протоколів і надає широкі можливості керування дзвінками, такими як:

- голосова пошта;
- конференц-зв'язок;
- IVR (інтерактивне голосове меню);
- центр обробки дзвінків;
- Call Detail Record (детальний звіт про дзвінки).

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. Завдяки вільній ліцензії Asterisk активно розвивається і підтримується тисячами людей з усього світу.

Для істаляції та запуску Asterisk, ми будемо використовувати дистрибутив на базі ядрі лінукс Ubuntu 16.04. Виконання більшості команд потребуватиме прав суперкористувача root. Можна запускати команди з вказанням команди sudo, або ж змінити режим користувача sudo su (рисунок 3.2).

Перейдемо в директорію /usr/src в якій ми розмістимо наш asterisk:

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

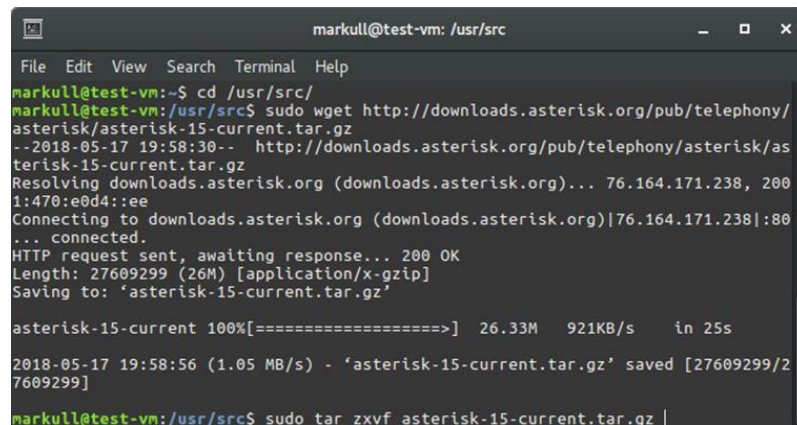
Завантажемо tar.gz файл останньої версії Asterisk 15.4.0 командою wget

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						51
Змн.	Арк.	№ докум.	Підпис	Дата		

```
$ sudo wget http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-15-current.tar.gz
```

Розпакуємо архів командою tar:

```
$ sudo tar zxvf asterisk-15-current.tar.gz
```



```
markull@test-vm: /usr/src
File Edit View Search Terminal Help
markull@test-vm:~$ cd /usr/src/
markull@test-vm:/usr/src$ sudo wget http://downloads.asterisk.org/pub/telephony/
asterisk/asterisk-15-current.tar.gz
--2018-05-17 19:58:30-- http://downloads.asterisk.org/pub/telephony/asterisk/as
terisk-15-current.tar.gz
Resolving downloads.asterisk.org (downloads.asterisk.org)... 76.164.171.238, 200
1:470:e0d4:ee
Connecting to downloads.asterisk.org (downloads.asterisk.org)[76.164.171.238]:80
... connected.
HTTP request sent, awaiting response... 200 OK
Length: 27609299 (26M) [application/x-gzip]
Saving to: 'asterisk-15-current.tar.gz'

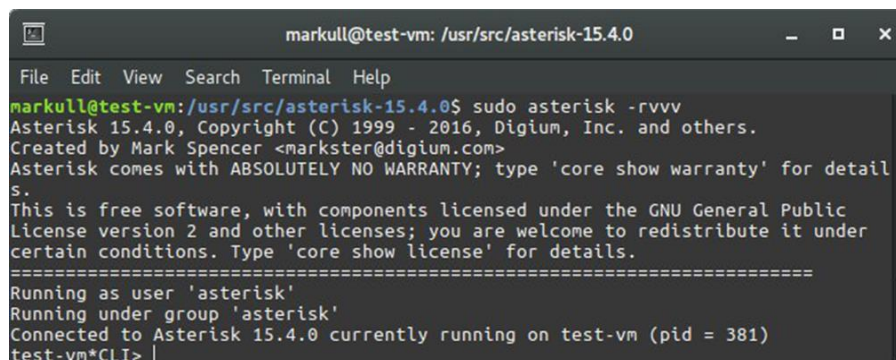
asterisk-15-current 100%[=====] 26.33M 921KB/s in 25s

2018-05-17 19:58:56 (1.05 MB/s) - 'asterisk-15-current.tar.gz' saved [27609299/2
7609299]
markull@test-vm:/usr/src$ sudo tar zxvf asterisk-15-current.tar.gz |
```

Рисунок 3.2 - Виконання команд в терміналі

Запускаємо Asterisk (рисунок 3.3):

```
$ sudo asterisk -rvvv
```



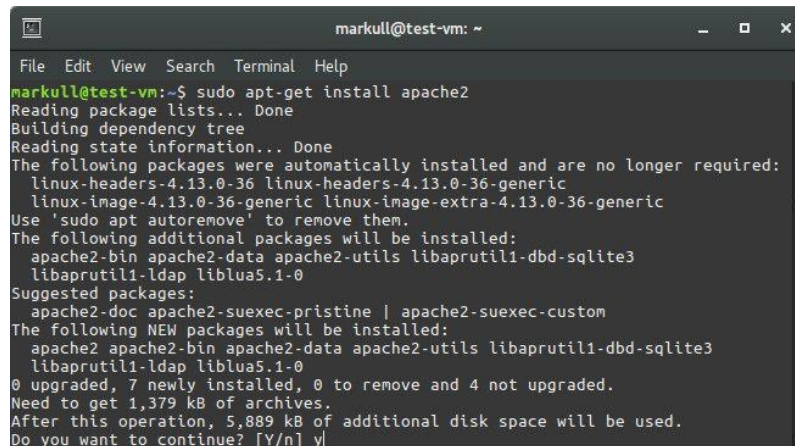
```
markull@test-vm: /usr/src/asterisk-15.4.0
File Edit View Search Terminal Help
markull@test-vm:/usr/src/asterisk-15.4.0$ sudo asterisk -rvvv
Asterisk 15.4.0, Copyright (C) 1999 - 2016, Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for detail
s.
This is free software, with components licensed under the GNU General Public
license version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Running as user 'asterisk'
Running under group 'asterisk'
Connected to Asterisk 15.4.0 currently running on test-vm (pid = 381)
test-vm*CLI> |
```

Рисунок 3.3 - Запуск Asterisk

Установка та налаштування FreePBX 14.0. Для встановлення FreePBX необхідно спершу встановити і налаштувати Apache2, MySQL, PHP5.6 (! FreePBX може некоректно працювати з версією 7.0).

Встановлюємо apache2 (рисунок 3.4):

```
$ sudo apt-get install apache2
```



```
markull@test-vm: ~  
File Edit View Search Terminal Help  
markull@test-vm:~$ sudo apt-get install apache2  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  linux-headers-4.13.0-36 linux-headers-4.13.0-36-generic  
  linux-image-4.13.0-36-generic linux-image-extra-4.13.0-36-generic  
Use 'sudo apt autoremove' to remove them.  
The following additional packages will be installed:  
  apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3  
  libaprutil1-ldap liblua5.1-0  
Suggested packages:  
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom  
The following NEW packages will be installed:  
  apache2 apache2-bin apache2-data apache2-utils libaprutil1-dbd-sqlite3  
  libaprutil1-ldap liblua5.1-0  
0 upgraded, 7 newly installed, 0 to remove and 4 not upgraded.  
Need to get 1,379 kB of archives.  
After this operation, 5,889 kB of additional disk space will be used.  
Do you want to continue? [Y/n] y
```

Рисунок 3.4 - Встановлення apache2

Відкриємо початкову сторінку Apache в браузері, підключившись до localhost (рисунок 3.5).



Рисунок 3.5 - Відображення початкової сторінки Apache2 браузері

В файлі конфігурацій asterisk.conf видаляємо символи “(!)” навпроти [directories]. В протилежному випадку, при встановленні freePBX вискочить помилка

						Арк.
						53
Змн.	Арк.	№ докум.	Підпис	Дата	ДП.КСМ.111862/16.00.00.000 ПЗ	

читання файлу asterisk.conf. Для редагування файлу можна скористатись редактором nano (або будь-яким іншим)

Завантажуємо та розархівуємо FreePBX 14 (рисунок 3.6):

```
$ wget http://mirror.freepbx.org/modules/packages/freepbx/freepbx-14.0-latest.tgz
```

```
$ tar -xzf freepbx-14.0-latest.tgz
```



```
markull@test-vm: ~/Downloads
File Edit View Search Terminal Help
markull@test-vm:~/Downloads$ wget http://mirror.freepbx.org/modules/packages/freepbx/freepbx-14.0-latest.tgz
--2018-05-23 01:03:44-- http://mirror.freepbx.org/modules/packages/freepbx/freepbx-14.0-latest.tgz
Resolving mirror.freepbx.org (mirror.freepbx.org)... 199.102.239.170
Connecting to mirror.freepbx.org (mirror.freepbx.org)|199.102.239.170|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14765548 (14M) [application/octet-stream]
Saving to: 'freepbx-14.0-latest.tgz'

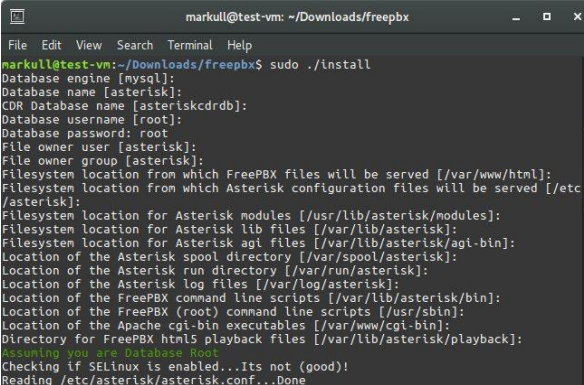
freepbx-14.0-latest 100%[=====] 14.08M 2.39MB/s in 6.9s

2018-05-23 01:03:51 (2.03 MB/s) - 'freepbx-14.0-latest.tgz' saved [14765548/14765548]
markull@test-vm:~/Downloads$ tar -xzf freepbx-14.0-latest.tgz
markull@test-vm:~/Downloads$
```

Рисунок 3.6 – Завантаження FreePBX

Запускаємо скрипт встановлення FreePBX (рисунок 3.7):

```
$ sudo ./install
```



```
markull@test-vm: ~/Downloads/freepbx
File Edit View Search Terminal Help
markull@test-vm:~/Downloads/freepbx$ sudo ./install
Database engine [mysql]:
Database name [asterisk]:
CDR Database name [asteriskcdrdb]:
Database username [root]:
Database password: root
File owner user [asterisk]:
File owner group [asterisk]:
Filesystem location from which FreePBX files will be served [/var/www/html]:
Filesystem location from which Asterisk configuration files will be served [/etc/asterisk]:
Filesystem location for Asterisk modules [/usr/lib/asterisk/modules]:
Filesystem location for Asterisk lib files [/var/lib/asterisk]:
Filesystem location for Asterisk agi files [/var/lib/asterisk/agi-bin]:
Location of the Asterisk spool directory [/var/spool/asterisk]:
Location of the Asterisk run directory [/var/run/asterisk]:
Location of the Asterisk log files [/var/log/asterisk]:
Location of the FreePBX command line scripts [/var/lib/asterisk/bin]:
Location of the FreePBX (root) command line scripts [/usr/sbin]:
Location of the Apache cgi-bin executables [/var/www/cgi-bin]:
Directory for FreePBX html5 playback files [/var/lib/asterisk/playback]:
Assuming you are Database Root
Checking if SELinux is enabled...Its not (good)!
Reading /etc/asterisk/asterisk.conf...Done
```

Рисунок 3.7 – Встановлення FreePBX

Підключаємось до FreePBX в браузері localhost/admin/config.php (рисунок 3.8).

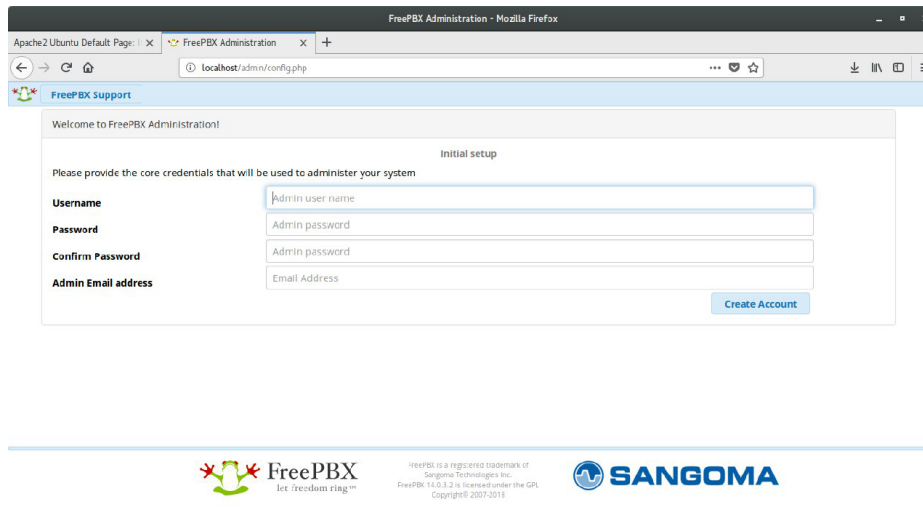


Рисунок 3.8 - Відображення початкової сторінки freepbx в браузері

На цьому налаштування Asterisk та FreePBX завершено. Команди налаштування Asterisk та FreePBX наведено у додатку А.

3.4 Моделювання телефонної мережі компанії

Перш ніж перейти до втілення ідеї розробки в життя, потрібно її спроектувати. Для цього було вибрано програму-симулятор “CISCO Packet Tracer 7”. На рисунку 3.9 зображено побудову локальної мережі згідно логічної топології компанії.

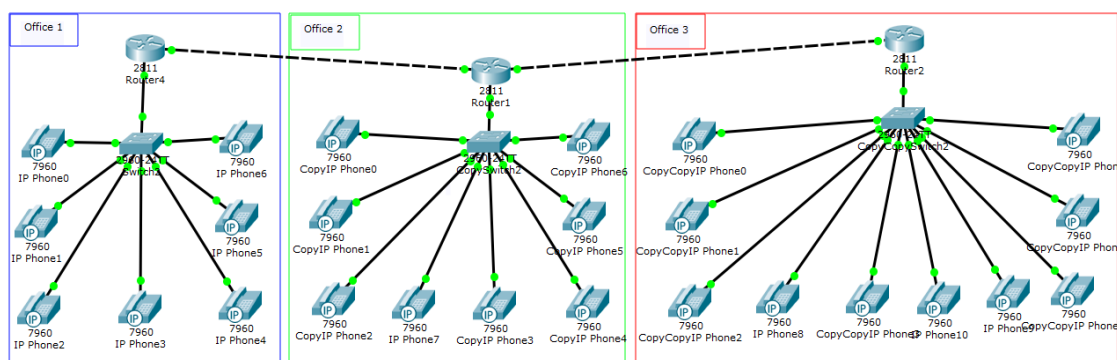


Рисунок 3.9 — Загальний вигляд локальної мережі компанії

В даному випадку було спроектовано мережу IP-телефонів в межах трьох офісів засобами IP-телефонії.

IP-телефонія — це технологія, що дозволяє використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передачі відеозображень та факсів у режимі реального часу.

При відправленні або отриманні електронної пошти відбувається передача «пакета» інформації через мережу Інтернет. Аналогічним чином працює й IP-телефонія. Створення «пакетів» — перетворення аналогових (зокрема, звукових) сигналів у цифрові, їх стискання, передачу мережею Internet і зворотне перетворення в аналогові відбувається завдяки існуванню протоколу передачі даних через Інтернет (IP — Internet Protocol), звідси і назва «IP-телефонія».

Основною перевагою IP-телефонії є нижча вартість міжміських і міжнародних переговорів у порівнянні з традиційною телефонією за рахунок цифрування і наступної компресії (стиснення) голосового потоку, що дозволяє знизити собівартість послуги.

Друге — нижча вартість кінцевого устаткування. На шляху проходження пакетів інформації з голосовим сигналом не використовується дороге устаткування, що стало вже традиційним для міжнародної та міжміської телефонії. У цій високоякісній технології використовуються відносно недорогі комутатори-маршрутизатори.

3.4.1 Налаштування комутаторів

Після проектування топології слід перейти до налаштування обладнання. Цей процес починався з налаштування комутаторів та VLAN.

Для початку були використані команди для задання ip-адреси підмережі.

Switch 2

Switch(config)#interface vlan 1

Switch(config-if)#ip address 10.3.0.100 255.255.255.0

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		56

```
Switch(config-if)#no shutdown
```

Результат представлено на рисунку 3.10.

```
GigabitEthernet0/1  Down  1  --  00E0.F93C.C119
GigabitEthernet0/2  Down  1  --  00E0.F93C.C11A
Vlan1               Up    1  10.3.0.100/24  0001.4284.5D18
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.10 — Задання IP-адреси для підмережі

Switch 3

```
Switch(config)#interface vlan 1
```

```
Switch(config-if)#ip address 20.4.0.100 255.0.0.0
```

```
Switch(config-if)#no shutdown
```

Результат представлено на рисунку 3.11.

```
-----
Vlan1               Up    1  20.4.0.100/24  0003.E463.BA1C
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.11 — Задання ip-адреси для підмережі

Switch 4

```
Switch(config)#interface vlan 1.
```

```
Switch(config-if)#ip address 40.6.0.100 255.0.0.0
```

```
Switch(config-if)#no shutdown
```

Результат представлено на рисунку 3.12.

```
GigabitEthernet0/2  Down  1  --  0060.5CCC.0C30
Vlan1               Up    1  40.6.0.100/24  0001.C9E1.C0B6
Hostname: Switch

Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet
```

Рисунок 3.12 — Задання ip-адреси для підмережі

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						57
Змн.	Арк.	№ докум.	Підпис	Дата		

Далі слід налаштувати голосові порти, оскільки мережа передбачає використання ір-телефонів.

Перелік використаних команд наведено нижче, а результат їх виконання на рисунку 3.13.

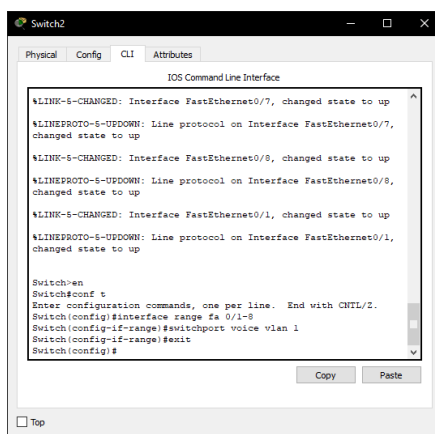


Рисунок 3.13 — Налаштування голосових портів комутатора №2

Switch2:

Switch>enable

Switch#conf te

Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)#interface range fa 0/1-8

Switch(config-if)#switchport voice vlan 1

Switch(config-if)#exit

Команда “interface range fa 0/1-8” дозволяє задати налаштування зразу для *n*-ої кількості портів (в даному випадку для портів з 1-го по 8-й, до яких підключено ІР-телефони), що значно пришвидшує налаштування модулів, для яких потрібно вводити одні і ті ж параметри.

Аналогічні дії було повторено на комутаторах №3 та №4 для портів 0/1-9 та 0/1-11 відповідно.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		58

3.4.2 Налаштування маршрутизаторів

Наступним кроком після налаштування комутаторів є налаштування маршрутизаторів (рисунок 3.14). Для початку, по аналогії з комутаторами, портам передачі даних присвоювались їх IP-адреси за допомогою таких команд:

- interface fa */* — команда вибору порта, де «*» — його номер;
- ip address «ір-адреса» «маска підмережі» — задання адреси та маски;
- no shutdown — перемикання стану порта на «активний».

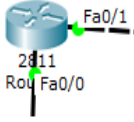
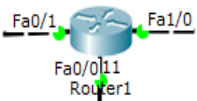
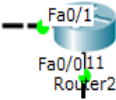
Port	Link	VLAN	IP Address	IPv6 Address	
FastEthernet0/0	Up	--	10.3.0.1/24	<not set>	
FastEthernet0/1	Up	--	30.10.1.1/24	<not set>	
Vlan1	Down	1	<not set>	<not set>	
Hostname: Router					Router4
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					
Port	Link	VLAN	IP Address	IPv6 Address	
FastEthernet0/0	Up	--	20.4.0.1/24	<not set>	
FastEthernet0/1	Up	--	30.10.1.2/24	<not set>	
FastEthernet1/0	Up	--	30.10.2.1/24	<not set>	
FastEthernet1/1	Down	--	<not set>	<not set>	
Vlan1	Down	1	<not set>	<not set>	
Hostname: Router					Router1
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					
Port	Link	VLAN	IP Address	IPv6 Address	
FastEthernet0/0	Up	--	40.6.0.1/24	<not set>	
FastEthernet0/1	Up	--	30.10.2.2/24	<not set>	
Vlan1	Down	1	<not set>	<not set>	
Hostname: Router					Router2
Physical Location: Intercity, Home City, Corporate Office, Main Wiring Closet					

Рисунок 3.14 — Налаштування IP-адрес портів для Router4, Router1, Router2

В даній мережі маршрутизатори також будуть виконувати роль TFTP-серверів.

TFTP (англ. Trivial File Transfer Protocol — тривіальний протокол передачі файлів) — простий, покроково синхронізований протокол передачі файлів, який дозволяє клієнтам зчитувати або записувати файли сервера. Одним із основних використань протоколу є первинне завантаження бездискових робочих станцій у локальній мережі. Найчастіше TFTP використовується саме через простоту його реалізації. Протокол працює поверх протоколу UDP.

Тобто, з TFTP-сервера IP-телефони в даній мережі будуть отримувати свою прошивку (програмне забезпечення), ір-адреси та номери при завантаженні. Перелік команд наведено в таблиці 3.1.

Таблиця 3.1 — Команди створення пулу IP-адрес для IP-телефонів

	Router4	Router1	Router2
Команда	Параметри	Параметри	Параметри
Router(config)#ip dhcp excluded-address	10.3.0.1	20.4.0.1	40.6.0.1
Router(config)#ip dhcp pool	Phones	Phones	Phones
Router(dhcp-config)#network	10.3.0.0 255.255.255.0	20.4.0.1 255.255.255.0	40.6.0.1 255.255.255.0
Router(dhcp-config)#default-router	10.3.0.1	20.4.0.1	40.6.0.1
Router(dhcp-config)#option 150 ip	10.3.0.1	20.4.0.1	40.6.0.1

Дані команди виконують наступні функції: резервують IP-адреси портів для того, щоб IP-телефони не могли присвоїти собі їх адресу, створюють пул IP-адрес для телефонів, встановлюють стандартну точку входу/виходу даних у вигляді порта маршрутизатора.

Наступним кроком було налаштування телефонії. Нижче наведено перелік команд які визначають максимальну кількість телефонів в мережі, максимальну кількість визначених телефонних номерів, джерело їх видачі у вигляді маршрутизатора, автоматичне розподілення номерів та самі номери, наведено в таблиці 3.2. Номери 1-го офісу починаються цифрою «1», номери 2-го та третього офісів відповідно цифрами «2» та «3». Команди з «Router(config)#ephone-dn» по «Router(config-telephony)# exit» задають номер для кожного телефону, відповідно параметри цієї команди будуть мінятись у зростаючому порядку, наприклад: 101, 102, 103 і т.д. для 1-го офісу, 201, 202, 203 і т.д. для 2-го офісу і 301, 302, 303 і т.д. для 3-го офісу.

Таблиця 3.2 — Задання кількості ір-телефонів та розподіл номерів

Команда	Router4	Router1	Router2
	Параметри	Параметри	Параметри
1	2	3	4
Router(config)#	telephony-service	telephony-service	telephony-service

Продовження таблиці 3.2

1	2	3	4
Router(config-telephony)#max-ephones	7	8	10
Router(config-telephony)#max-dn	7	8	10
Router(config-telephony)#ip source-address	10.3.0.1 port 2000	20.4.0.1 port 2000	40.6.0.1 port 2000
Router(config-telephony)#auto assign	1 to 7	1 to 8	1 to 10
Router(config-telephony)#	exit	exit	exit
Router(config)#ephone-dn	1	1	1
Router(config-ephone-dn)#number	101	201	301
Router(config-telephony)#	exit	exit	exit

Таблиця 3.3 — Налаштування передачі даних між маршрутизаторами

	Router4		Router1		Router2	
Команда	Параметри		Параметри		Параметри	
Router(config)#ip route	0.0.0.0 0.0.0.0		0.0.0.0 0.0.0.0		0.0.0.0 0.0.0.0	
	30.10.1.2	30.10.2.2	30.10.1.1	30.10.2.2	30.10.1.1	30.10.2.1
Router(config)#ip route	10.3.0.1 255.255.255.255		20.4.0.1 255.255.255.255		40.6.0.1 255.255.255.255	
	30.10.1.2	30.10.2.2	30.10.1.1	30.10.2.2	30.10.1.1	30.10.2.1
Router(config)#dial-peer voice	1 voip	2 voip	1 voip	2 voip	1 voip	2 voip
Router(config-dial-peer)#destination-pattern	2..	3..	1..	3..	1..	2..
Router(config-dial-peer)#session target ipv4:	30.10.1.2	30.10.2.2	30.10.1.1	30.10.2.2	30.10.1.1	30.10.2.1

Останнім кроком в налаштуванні маршрутизаторів (таблиці 3.3) було встановлення мостів між ними, налаштування вихідної точки виклику POTS, вказання шаблону номерів, який повинен набрати користувач, щоб здійснити виклик, який включає префікс і номер призначення, призначення адресу певної

мережі для отримання дзвінків від точки виклику VoIP. Вище наведено перелік команд використаних для даних цілей.

3.5 Перевірка працездатності мережі

Останнім етапом розробки мережі компанії є перевірка роботи усіх вузлів та усунення можливих помилок.

Для цього було перевірено коректність роботи IP-телефонів, шляхом режиму симуляції дзвінка. Спочатку було перевірено зв'язок між IP-телефонами однієї підмережі “Office 1”, “Office 2” та “Office 3”, представлено на рисунках 3.15 -3.17.

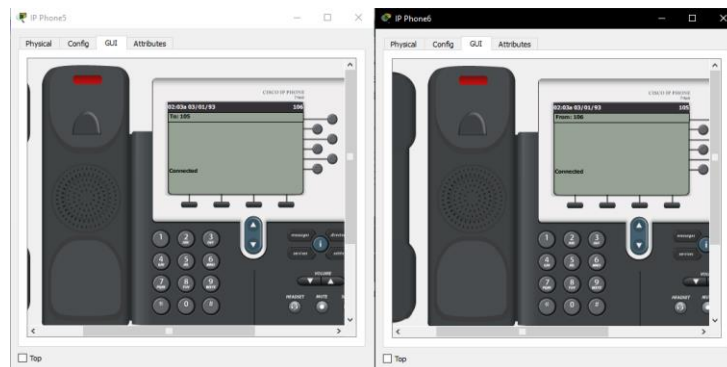


Рисунок 3.15 —Перевірка виклику між IP-телефонами підмережі “Office 1”



Рисунок 3.16—Перевірка виклику між IP-телефонами підмережі “Office 2”



Рисунок 3.17 —Перевірка виклику між IP-телефонами підмережі “Office 3”

Наведені вище скріншоти свідчать про те, що виклик було здійснено між IP-телефонами з номерами 106 – 105 (підмережа 1-го офісу), 202 – 208 (підмережа 2-го офісу) та 307 – 304 (підмережа 3-го офісу), а напис “Connected” (з’єднано) на екранах IP-телефонів підтверджує встановлене з’єднання між ними. Далі було перевірено зв’язок між IP-телефонами різних підмереж аналогічним способом, представлено на рисунках 3.18 – 3.20.

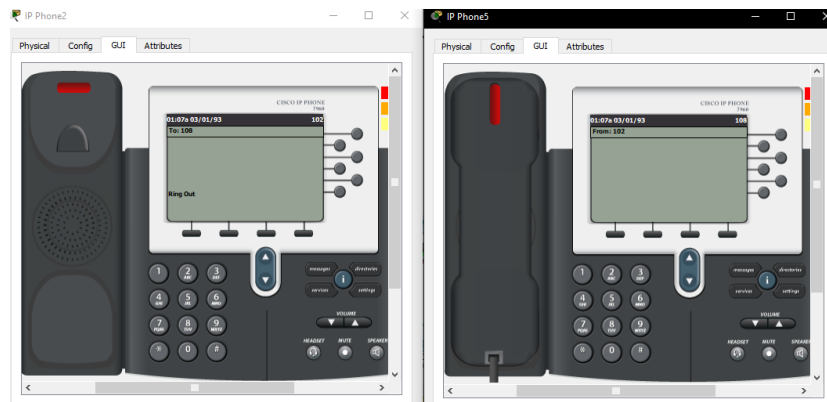


Рисунок 3.18 —Перевірка виклику між підмережами 1-го та 2-го офісів



Рисунок 3.19 —Перевірка виклику між підмережами 2-го та 3-го офісів



Рисунок 3.20 —Перевірка виклику між підмережами 1-го та 3-го офісів

На рисунках 3.18 – 3.20 результати аналогічні попереднім, а це означає, що IP-телефони та прохідні порти на комутаторах і маршрутизаторах було налаштовано вірно і IP-телефони всіх трьох офісів можуть вільно здійснювати дзвінки між собою.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		64

4 ТЕХНІКО-ЕКОНОМІЧНИЙ РОЗДІЛ

Метою техніко-економічного розділу є здійснення економічних розрахунків, спрямованих на визначення економічної ефективності розробки проекту мережі для підприємства і прийняття рішення про його подальший розвиток і впровадження або ж недоцільність проведення відповідної розробки.

Для визначення загальної тривалості проведення НДР дані витрат часу з окремих операцій доцільно звести у таблицю 4.1.

4.1 Визначення витрат на оплату праці та відрахувань на соціальні заходи

Витрати на оплату праці включають заробітну плату (ЗП) всіх категорій працівників, безпосередньо зайнятих на всіх етапах проектування. Розмір ЗП обчислюється на основі трудоемності відповідних робіт та середньої ЗП відповідних категорій працівників.

У розробці проектного рішення задіяні наступні спеціалісти - розробники, а саме: керівник проекту; студент-дипломник; консультант техніко-економічного розділу (таблиця 4.1).

Таблиця 4.1 - Вихідні дані для розрахунку витрат на оплату праці

Посада виконавців	Місячний оклад (стипендія), грн.
Керівник ДП, викладач	4916,00
Консультант техніко-економічного розділу, доцент	6026,00
Студент	1100,00

Витрати на оплату праці розробників проекту визначаються за формулою:

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		65

$$B_{OP} = \sum_{i=1}^N \sum_{j=1}^M n_{ij} \cdot t_{ij} \cdot C_{ij}, \quad (4.1)$$

де n_{ij} – чисельність розробників i -ої спеціальності j -го тарифного розряду, осіб;

t_{ij} – затрачений час на розробку проекту співробітником i -ої спеціальності j -го тарифного розряду, год;

C_{ij} – годинна ставка працівника i -ої спеціальності j -го тарифного розряду, грн.,

Середньо годинна ставка працівника може бути розрахована за формулою:

$$C_{ij} = \frac{C_{ij}^0(1+h)}{PЧ_i}, \quad (4.2)$$

де C_{ij} – основна місячна заробітна плата розробника i -ої спеціальності j -го тарифного розряду, грн.;

h – коефіцієнт, що визначає розмір додаткової заробітної плати (при умові наявності доплат);

$PЧ_i$ - місячний фонд робочого часу працівника i -ої спеціальності j -го тарифного розряду, год. (приймаємо 168 год.).

Коефіцієнт h , який визначає розмір додаткової заробітної плати, для керівника та консультанта техніко-економічного розділу дорівнює 1,47.

Середня годинна ставка керівника ДП дорівнює:

$$C_{ij} = \frac{4916 \cdot (1+1,47)}{168} = 72,28 \text{ грн/год.}$$

Середня годинна ставка консультанта техніко-економічного розділу ДП дорівнює:

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						66
Змн.	Арк.	№ докум.	Підпис	Дата		

$$C_{ij} = \frac{6026 \cdot (1 + 1,47)}{168} = 88,60 \text{ грн/год.}$$

Середня годинна оплата студента дорівнює:

$$C_{ij} = \frac{1100}{168} = 6,55 \text{ грн/год.}$$

Звідси, загальні витрати на оплату праці ($B_{ОП}$) дорівнюють:

$$B_{ОП} = 16 \cdot 72,28 + 144 \cdot 6,55 + 2 \cdot 88,60 = 2276,88 \text{ грн.}$$

Дані для розрахунку витрат на оплату праці наведено в таблиці 4.2

Таблиця 4.2 - Середній час виконання НДР та стадії (операції) технологічного процесу

Назва операції (стадії)	Середній час виконання операції, год.	Погодинна заробітна плата, грн/год.	Витрати на розробку, грн
Керівник ДП, викладач	16	72,28	1156,48
Консультант ТЕР, доцент	2	88,60	177,20
Розробка проекту мережі, студент	144	6,55	943,20
Разом			2276,88

Крім того, слід визначити відрахування на соціальні заходи. Величну відрахувань у спеціальні державні фонди визначають у відсотковому співвідношенні від суми основної та додаткової заробітних плат. Згідно діючого нормативного законодавства сума відрахувань у спеціальні державні фонди складає 20,5% від суми заробітної плати:

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						67
Змн.	Арк.	№ докум.	Підпис	Дата		

$$B_{\phi} = 0,205 \cdot B_{\text{ОП}},$$

$$B_{\phi} = \frac{20,5}{100} \cdot 2276,88 = 466,76 \text{ грн.}$$

Загальна сума витрат на матеріальні ресурси (B_M) визначається за формулою:

$$B_M = \sum_{i=1}^n K_i \cdot C_i, \quad (4.3)$$

де K_i - витрата i -го типу матеріалу, натуральні одиниці вимірювання;

C_i - ціна за одиницю i -го типу матеріалу, грн.;

i - тип матеріального ресурсу;

n - кількість типів матеріальних ресурсів

Звідси, витрати на матеріальні ресурси дорівнюватимуть:

$$B_M = 9285,00 + 5319,00 + 700,00 + 8200,00 = 23504,00 \text{ грн.}$$

Проведені розрахунки занесемо у таблицю 4.3.

Таблиця 4.3 - Зведені розрахунки матеріальних витрат

Найменування матеріальних ресурсів	Од. виміру	Факт. витрачено матеріалів	Ціна за одиницю, грн.	Загальна сума, грн.
Сервер	шт.	1	9285,00	9285,00
IP-телефони	шт.	3	1773,00	5319,00
WI FI-маршрутизатор	шт.	1	700,00	700,00
Комутатор 48 портів	шт.	1	8200,00	8200,00
Разом		9		23504,00

Загальна сума витрат на електроенергію розраховується за формулою:

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		68

$$B_E = \sum_{i=1}^n P_i \cdot k_i \cdot T_i \cdot C, \quad (4.4)$$

де P_i - паспортна потужність i -го електрообладнання, кВт;

k_i - коефіцієнт використання потужності i -го електрообладнання (приймається 0.7 , 0.9);

T_i - час роботи i -го обладнання за весь період розробки, год;

C - ціна електроенергії, грн / кВт·год;

i - тип електрообладнання;

n - кількість електрообладнання.

Для розробки проекту даної комп'ютерної мережі використовується один ПК потужністю $P = 0,22$ кВт з монітором потужністю $P = 0,013$ кВт, який за весь період розробки працює 21 годину, та друкуючий пристрій потужністю $P = 0,37$ кВт, який працює 2 години.

$$B_E = 0,9 \cdot (0,22 + 0,013) \cdot 21 \cdot 0,9 + 0,9 \cdot 0,37 \cdot 2 \cdot 0,9 = 5,16 \text{ грн.}$$

Амортизація – це процес перенесення вартості основних фондів на вартість новоствореної продукції з метою їх повного відновлення.

Для визначення амортизаційних відрахувань застосуємо метод прямолінійного списання. Загальна сума амортизаційних відрахувань (B_{AM}) визначається за формулою:

$$B_{AM} = \sum_{i=1}^n \frac{B_i \cdot H_i}{100}, \quad (4.5)$$

де B_i - вартість i -го обладнання на початок звітного періоду, грн.;

H_i - річна норма амортизації i -го обладнання, %;

i - тип обладнання;

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						69
Змн.	Арк.	№ докум.	Підпис	Дата		

n - кількість обладнання.

Для проектування даної комп'ютерної мережі використовуються один ноутбук вартістю 9500 грн., та принтер вартістю 3850 грн.

Тоді:

$$B_{AM} = \frac{9500 \cdot 10}{100} + \frac{3850 \cdot 20}{100} = 1720,00 \text{ грн.}$$

Транспортні витрати слід прогнозувати у розмірі 8–12 % від загальної суми матеріальних витрат.

$$B_T = 0.08 \cdot B_M, \quad (4.6)$$

де B_T – транспортні витрати.

$$B_T = 0,08 \cdot 23504,00 = 1880,32 \text{ грн.}$$

В залежності від організаційно-правової форми діяльності господарюючого суб'єкта, накладні витрати можуть становити 60–100 % від суми основної та додаткової заробітної плати працівників.

$$H_B = 0,7 \cdot B_{OP}, \quad (4.7)$$

де H_B – накладні витрати.

$$H_B = 0,7 \cdot 2276,88 = 1593,82 \text{ грн.}$$

Загальні витрати ($B_{КС}$) розраховуємо за формулою:

$$B_{КС} = B_{OP} + B_{\Phi} + B_M + B_E + B_{AM} + B_T + H_B \quad (4.8)$$

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						70
Змн.	Арк.	№ докум.	Підпис	Дата		

Результати проведених розрахунків зведемо у таблицю 4.4.

Таблиця 4.4 - Кошторис витрат

Зміст витрат	Сума, грн.
Витрати на оплату праці (осн. і дод. ЗП)	2276,88
Відрахування на соціальні заходи	466,76
Матеріальні витрати	23504,00
Витрати на електроенергію	5,16
Амортизаційні відрахування	1720,00
Транспортні витрати	1880,32
Накладні витрати	1593,82
РАЗОМ по кошторису	31446,94

4.2 Розрахунок ціни проекту

Договірна ціна (C_D) для проектних рішень розраховується за формулою:

$$C_D = B_{КС} \cdot \left(1 + \frac{P}{100}\right), \quad (4.9)$$

де $B_{КС}$ – кошторисна вартість, грн.;

p - середній рівень рентабельності, % (приймаємо 27% за погодженням з керівником).

$$C_D = 31446,94 \cdot (1 + 0,27) = 39937,61 \text{ грн.}$$

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		71

4.3 Визначення економічної ефективності і терміну окупності капітальних вкладень

Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = \frac{\Pi}{B_{КС}}, \quad (4.10)$$

де Π – прибуток, грн.;

$B_{КС}$ – кошторисна вартість, грн..

$$E_p = 8490,67 \text{ грн.} / 31446,94 \text{ грн.} = 0,27.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = \frac{1}{E_p}. \quad (4.11)$$

Тобто:

$$T_p = 1/0,27 = 3,7 \text{ р.}$$

Прийнятним вважається термін окупності близький до 7 років.

Розраховані економічні показники проекту занесемо до таблиці 4.5.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
						72
Змн.	Арк.	№ докум.	Підпис	Дата		

Таблиця 4.5 - Економічні показники розробки

Показник	Значення
Собівартість, грн.	31446,94
Плановий прибуток, грн.	8490,67
Ціна, грн.	39937,61
Економічна ефективність	0,27
Термін окупності, рік	3,7

Враховуючи основні економічні показники з таблиці 4.5, можна зробити висновок, що при економічній ефективності 0,27 та терміні окупності – 3,7 років проводити роботи по впровадженню даної мережі є доцільним та економічно вигідним. Як можна побачити із розрахунків, основними є матеріальні витрати. Тому, з метою зниження вартості мережі, варто було б здійснювати закупівлю обладнання у офіційних дилерів вказаних марок обладнання.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		73

ВИСНОВКИ

В даному дипломному проекті була розроблена і запущена в роботу корпоративна мережа і корпоративний телефонний зв'язок, що задовольняє всі запити компанії

1. Проведено порівняння основних підходів до створення корпоративної телефонної мережі.

2. Проведено аналіз основних протоколів IP-телефонії, виділено їх основні переваги. В результаті аналізу для проектування телефонної мережі було обрано протокол SIP.

3. Здійснено вибір обладнання для проектованої мережі. Обрано обладнання компанії Cisco.

4. Запропоновано рішення для телефонної мережі філії, які включають наступні етапи: перехід з протоколу H.323 на SIP, заміна обладнання, зміна схеми включення шлюзу внутрішньої мережі та перехід на статичну маршрутизацію викликів у внутрішній мережі, організація зв'язку з корпоративною мережею.

5. Запропоновано спосіб сполучення VoIP-мережі із телефонною мережею загального користування. В результаті чого було налагоджено взаємодію з іншими мережами сполучення SIP-H.323. Взаємодію виконано через зв'язку двох шлюзів SIPTDM-H.323

6. Проведено налаштування Asterisk-сервера на ОС Linux.

7. Проведено моделювання VoIP-мережі. В процесі виконання було промодельовано мережу, яка складається із трьох розділених офісів, налаштовано комутатори та маршрутизатори та проведено перевірку роботи системи IP-телефонії, як в межах одного офісу, так і між офісами.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		74

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гольштейн Б.С.. Учебник для вузов: «Системы коммутации» / Б.С. Гольштейн // С-Пб.:БХВ-Санкт-Петербург, 2003.-318 с.:ил.
2. Руководство по Cisco IOS [Текст]. - СПб.: Питер, М.: Издательство «Русская Редакция», 2008. -784 с
3. Официальный сайт производителя оборудования Cisco Systems [Электронный ресурс] / Режим доступа – <http://www.cisco.com>.
4. Хьюкаби, Д. Руководство по конфигурированию коммутаторов Catalyst.: Пер. с англ. [Текст]/ Д. Хьюкаби, С. Мак-Квери– М.: Издательский дом «Вильямс» – 2004. – 560 с.
5. Основы организации сетей Cisco, том 1 [Текст].: Пер. с англ. - М.: Издательский дом «Вильямс», 2002. - 512 с.
6. Портнов, Э.Л. Оптические кабели связи [Текст] / Э.Л. Портнов– М. «Информсвязь», 2000 – 112 с.
7. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство, 3-е изд., с испр. [Текст]: Пер. с англ. – М.: ООО «И. Д. Вильямс», 2007. – 994.
8. Величко В.В. Телекоммуникационные системы и сети: Учебное пособие в 3-х томах. Том 3. – Мультисервисные сети [Текст] / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев; под ред. профессора В.П. Шувалова. – М.: Горячая линия – Телеком, 2005. – 592 с.
9. Росляков А.В. IP-телефония / А.В. Росляков, М.Ю. Самсонов, И.В. Шибаева– М.: Эко-Трендз, 2003. – 252 с.
10. Гольштейн Б.С. IP-телефония / Б.С. Гольштейн, А.В. Пинчук, А. Л. Суховицкий // М.: Радио связь, 2001.- 366с.:ил.
11. Гольштейн Б.С. Справочник по телекоммуникационным протоколам: «Протокол SIP» / Б.С. Гольштейн, А. А. Зарубин, В. В. Саморезов // С-Пб.:БХВ-Санкт-Петербург, 2005.-456с.:ил.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		75

12. Принципы маршрутизации в Internet, 2-е издание [Текст]: Пер. с англ. М.: Издательский дом "Вильямс", 2001. - 448 с.: ил.
13. Руководство по Cisco IOS [Текст]. - СПб.: Питер, М.: Издательство «Русская Редакция», 2008. -784 с
14. Официальный сайт производителя оборудования Cisco Systems [Электронный ресурс] / Режим доступа – <http://www.cisco.com>.
15. Хьюкаби, Д. Руководство по конфигурированию коммутаторов Catalyst.: Пер. с англ. [Текст]/ Д. Хьюкаби, С. Мак-Квери– М.: Издательский дом «Вильямс» – 2004. – 560 с.
16. Транспортные сети и системы электросвязи. Системы мультиплексирования: Учебник для студентов ВУЗов по специальности «Телекоммуникации» [Текст] / Под ред. В.К. Стеклова. – К.; 2003 – 352 с.
17. Дональд, Дж. Стерлинг. Техническое руководство по волоконной оптике [Текст] / Дональд Дж. Стерлинг., пер. Московченко А. – Издательство «ЛОРИ» – 1998.
18. Основы организации сетей Cisco, том 1 [Текст].: Пер. с англ. - М.: Издательский дом «Вильямс», 2002. - 512 с.
19. Портнов, Э.Л. Оптические кабели связи [Текст] / Э.Л. Портнов– М. «Информсвязь», 2000 – 112 с.
20. Программа сетевой академии Cisco CCNA 3 и 4. Вспомогательное руководство, 3-е изд., с испр. [Текст]: Пер. с англ. – М.: ООО «И. Д. Вильямс», 2007. – 994.
21. Слепов Н.Н. Оптиволоконные системы дальней связи. Перспективы развития [Текст] // Н.Н. Слепов. - Электроника: НТБ – 2005. – Вып.6.
22. Величко В.В. Телекоммуникационные системы и сети: Учебное пособие в 3-х томах. Том 3. – Мультисервисные сети [Текст] / В.В. Величко, Е.А. Субботин, В.П. Шувалов, А.Ф. Ярославцев; под ред. профессора В.П. Шувалова. – М.: Горячая линия – Телеком, 2005. – 592 с.
23. Методичні рекомендації до виконання дипломного проекту з освітньо-кваліфікаційного рівня “Бакалавр” напряму підготовки 6.050102

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		76

«Комп'ютерна інженерія» фахового спрямування «Комп'ютерні системи та мережі» / О.М. Березький, Л.О.Дубчак, Р.Б. Трембач, Г.М. Мельник, Ю.М. Батько, С.В. Івасьєв / Під ред. О.М. Березького. -Тернопіль: ТНЕУ, 2016. – 60 с.

24. Методичні вказівки до написання техніко-економічного розділу дипломних проектів освітньо-кваліфікаційного рівня «бакалавр» напряму підготовки 6.050102 комп'ютерна інженерія/ І.Р. Паздрій – Тернопіль: ТНЕУ, 2014. – 37 с.

					ДП.КСМ.111862/16.00.00.000 ПЗ	Арк.
Змн.	Арк.	№ докум.	Підпис	Дата		77