Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повне найменування інституту, факультету)

Кафедра телекомунікацій
(повна назва кафедри)

До захисту допущено
В.о. завідувача кафедри
_____ Валерій ЯВІСЯ
(підпис) (Ім'я, прізвище)
"___"_____2020_р.

Дипломна робота

на здобуття освітнього ступеня "бакалавр"
(назва ОС)

Спеціальність 172 Телекомунікації та радіотехніка,
(код і назва)

на тему: Побудова мережі all-IP на базі концепції IMS.

Виконав : студент _VI_ курсу, групи _ТЗ-62_____
(шифр групи)

_____ Полуденний Олександр Миколайович
(прізвище, ім'я, по батькові) (підпис)

Керівник _____ старший викладач Петрова В. М.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Консультант _____ Романов О. І., д.т.н. професор
(назва розділу) (посада, вчене звання, науковий ступінь, прізвище, ініціали) (підпис)

Рецензент _____ к.т.н., доцент Созонник Г. Д.
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.

Студент _____
(підпис)

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»

Інститут телекомунікаційних систем
(повна назва)

Кафедра телекомунікацій
(повна назва)

Освітній ступінь бакалавр

Спеціальність 172 Телекомунікації та радіотехніка
(код і назва)

ЗАТВЕРДЖУЮ

В.о. завідувача кафедри

_____ Валерій_ЯВІСЯ
(підпис) (ім'я, прізвище)

"_22 "_січня_2020 р.

З А В Д А Н Н Я
НА ДИПЛОМНУ РОБОТУ СТУДЕНТУ

Полуденному Олександру Миколайовичу
(прізвище, ім'я, по батькові)

1. Тема роботи Побудова мережі all-IP на базі концепції IMS.
керівник роботи старший викладач Петрова В. М.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від 30 березня 2020 р. №924-с
2. Термін подання студентом роботи 04.06.2020
3. Вихідні дані до роботи Концепція побудови мережі IMS. Функціональні компоненти: P-CSCF, I-CSCF, S-CSCF. Послуги LTE з використанням CSCF. Принцип передачі VoIP в мережі IMS
4.Зміст роботи
Вступ
Розділ 1. Еволюція розвитку телекомунікаційних мереж.
1.1. Аналіз побудови телекомунікаційних мереж на базі концепції NGN.
- Багаторівнева архітектура NGN.
- Технології використання на кожному рівні.
- Функції і архітектура Softswitch.
- Використання контролерів SBC.

1.2. Недоліки NGN.
1.3. Шляхи усунення недоліків - перехід до концепції IMS.
1.4. Історія розвитку IMS.
1.5 Висновки до розділу.
Розділ 2. Концепція мультимедійної підсистеми IMS.

2.1. Принцип побудови IP Multimedia Subsystem.
2.2. Функціональні компоненти, функціональні площини IMS.
2.3. Основні елементи IMS і їх функції.
2.4. Стандартизація IMS.
2.5. Актуальність використання IMS в LTE .
2.5. Послуги в IMS.
2.6 Висновки до розділу.
Розділ 3. Процес обслуговування абонентів в мережах IMS.
3.1. Реєстрація користувача в мережі IMS.

- Скасування реєстрації користувача в мережі IMS.
- Реєстрація множинних ідентифікаторів користувача.

3.2. Встановлення сеансу зв'язку в IMS
3.3. Висновки до розділу.
Розділ 4. VoIP Передача голосу. QoS заходи для мінімізації втрат пакетів. Аналіз продуктивності та збоїв з'єднання при передачі даних.

- Аналіз проблеми.
- Аналіз рішення для уникнення затримки в передачі.

4.3. Висновки до розділу.
Розділ 5. Оцінка безпеки IMS, дослідження вразливостей IMS.
5.2. Висновки до розділу.
Висновки
Список використаних джерел
5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)
1) Архітетура мережі IMS. 2) Структура рівня управління в мережі IMS. 3)Надання сервісів мережі LTE з використанням IMS. 4) Передача голосу по VoIP. 5)Вразливості мережі IMS.

6. Консультанти розділів роботи[1*]

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
2	Романов О. І., професор кафедри телекомунікацій	07.03.2020	20.03.2020
4	Романов О. І., професор кафедри телекомунікацій	06.04.2020	03.05.2020
5	Романов О. І., професор кафедри телекомунікацій	04.05.2020	25.05.2020

7. Дата видачі завдання 15.10.2019

КАЛЕНДАРНИЙ ПЛАН

[1*] Консультантом не може бути зазначено керівника дипломної роботи.

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Отримання індивідуального завдання. Збір інформації, що відповідає отриманому завданню.	15.10.2019-15.02.2020	
2	Аналіз побудови телекомунікаційних мереж на базі концепції NGN. Розгляд переваг і недоліків NGN. Дослідження шляхів усунення недоліків – перехід перехід до концепції IMS.	16.02.2020-6.03.2020	
3	Розгляд структури та роль мультисервісної IP підсистеми (IMS). Розгляд основних елементів IMS і їх функцій. Дослідження актуальності IMS в LTE і доступних послуг.	07.03.2020-20.03.2020	
4	Аналіз процесу реєстрації абонента в мережі IMS і встановлення сеансу зв’язку.	21.03.2020-5.04.2020	
5	Дослідження передачі голосу по VoIP. Аналіз продуктивності та QoS заходів для мінімізації втрат пакетів.	06.04.2020-03.05.2020	
6	Оцінка безпеки IMS, дослідження вразливостей IMS.	04.05.2020-25.05.2020	
7	Формулювання висновків.	25.05.2020-31.05.2020	
8	Оформлення дипломної роботи.	31.05.2020-03.06.2020	

Студент _____ Полуденний О. М.
(підпис) (прізвище та ініціали)

Керівник роботи _____ Петрова В. М.
(підпис) (прізвище та ініціали)

РЕФЕРАТ

Темою дипломної роботи роботи є побудова мережі all-IP на базі концепції IMS.

Робота містить 63 сторінки, зокрема 28 рисунків, 2 таблиці та 19 джерел інформації.

Актуальність теми обумовлена розвитком та застосуванням мультимедійної IP підсистеми IMS та її конвергенція з мобільними мережами 4G. Концепція мультимедійної підсистеми IP (IMS) описує мережеву архітектуру, основою якої є пакетна транспортна мережа, що підтримує всі технології доступу і надає велику кількість інфокомунікаційних послуг. Споживачеві перехід на IMS обіцяє появу персоналізованих послуг, заснованих на передачі графіки, відео, тексту і мови в будь-якій послідовності, залучення нових сервісів, а також поєднання та покращення існуючих.

Мета даної роботи полягає в аналізі концепції IP Multimedia Subsystem (IMS) , огляді технологій, які використовувалися при створенні концепції, які використовують зараз та підтвердженні можливостей надання нових послуг абонентам інфокомунікаційної мережі, при реалізації архітектури IMS.

В даній роботі розглядається еволюція розвитку телекомунікаційних мереж, концепція IMS, що має усі переваги NGN, але є більш сучасною та зручною для абонентів. Розглядається актуальність використання IMS в мережах LTE. Аналіз процес обслуговування абонентів в IMS. Передача голосу через Інтернет - протоколу (VoIP). Аналіз продуктивності, QoS заходи для мінімізації втрат пакетів і ідентифікації збоїв з'єднання під час передачі. Оцінка безпеки IMS, дослідження вразливості мережі IMS.

Abstract

The relevance of the topic is due to the development and application of multimedia IP subsystem IMS and its convergence with 4G mobile networks. The concept of IP Multimedia Subsystem (IMS) describes a network architecture, the main element of which is a packet transport network that supports all access technologies and provides implementation of a large number of infocommunication services. For consumers, switching to IMS promises personalized services based on the transmission of speech, text, graphics and video in any combination, creating new services, as well as combining and improving existing ones.

The purpose of this work is to analyze the concept of IP Multimedia Subsystem (IMS), review the technologies that were used in creating the concept, which are used now, and confirm the possibility of providing new services to subscribers of the infocommunication network, when implementing the IMS architecture.

This paper examines the evolution of telecommunications networks, the concept of IMS, which has all the advantages of NGN, but is more modern and convenient for subscribers. The relevance of using IMS in LTE networks is considered. Analysis of the customer service process in IMS. Voice transmission over the Internet Protocol (VoIP). Performance analysis, QoS measures to minimize packet loss and identify connection failures during transmission. IMS security assessment, vulnerability study of the IMS network.

ЗМІСТ

Перелік скорочень

NGN	Next Generation Network
ISDN	Integrated Services Digital Network
MPLS	Multiprotocol Label Switching
ITU-T	International Telecommunication Union — Telecommunication sector
IETF	Internet Engineering Task Force
SIP	Session Initiation Protocol
MGCP	Media Gateway Control Protocol
IMS	IP Multimedia Subsystem
SBC	Session Border Controller
VoIP	Voice over Internet Protocol
NAT	Network Address Translation
3GPP	3rd Generation Partnership Project
GPRS	General Packet Radio Service
ETSI	European Telecommunications Standards Institute
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
QoS	Quality of service
SS	Software softswitch
UMTS	Universal Mobile Telecommunications System
API	Application Programming Interface
INAP	Intelligent Network Application Part
HSS	Home Subscriber Server
PSTN	Public Switched Telephone Network
CSCF	Call Session Control Function
RTP	Real-time Transport Protocol
TDM	Time Division Multiplexing
MGCF	Media Gateway Control Function
GSM	Global System for Mobile Communications
LTE	Long Term Evolution
SVRCC	Single Radio Voice Call Continuity
eTVRA	East Tennessee Volunteer Recognition Awards
ТМЗК	Телекомунікаційна мережа загального користування
АТМ	Автоматична телефонна мережа
АТС	Автоматична телефонна станція
МСЕ	Міжнародний стандарт електрозв'язку

ВСТУП

Концепція IP Multimedia Subsystem (IMS) описує нову мережеву архітектуру, основним елементом якої є пакетна транспортна мережа, що підтримує всі технології доступу і забезпечує реалізацію великого числа інфокомунікаційних послуг. Її авторство належить міжнародному партнерству Third Generation Partnership Project(3GPP), що об'єднав European Telecommunications Standardization Institute (ETSI) і кілька національних організацій стандартизації.

Історично до появи IMS призвело розвиток двох технологій: еволюція інтелектуальних платформ і розвиток технології Softswitch.

Концепція IMS виникла в результаті еволюції базової мережі стільникового рухомого зв'язку третього покоління UMTS, коли до мережі на базі технології Softswitch була додана область управління мультимедійними сеансами на базі протоколу SIP. Надалі ця концепція була взята за основу Комітетом ETSI-TISPAN для використання на мережах з різними технологіями доступу (WLAN / Wi-Fi, xDSL, LTE). Концепції Softswitch і IMS мають багато спільного: діляться на рівні (площини), надання всіх послуг здійснюється на базі IP-мережі, існує поділ функцій управління викликом і комутації. Але в концепції IMS з'являється нова функція - сервер для користувача даних HSS. Дані, що зберігаються в HSS, використовуються для реєстрації користувача в IMS, аутентифікації користувача, взаємодії з функціями обліку вартості, визначення профілів і параметрів послуг для даного користувача.

Концепція IMS може розглядатися як можливе рішення для побудови мереж наступного покоління і як основа конвергенції мобільних і стаціонарних мереж на платформі IP.

Розділ 1. Еволюція розвитку телекомунікаційних мереж.

У сучасному світі, який постійно розвивається, людство все більше відходить від аналогових технологій до цифрових. Це пов’язано з тим, що старі аналогові системи не можуть відповідати всім вимогам абонентів за обсягом, швидкістю та якістю передачі даних. Але нюанс також полягає в тому, що деякі абоненти не хотіли переходити на нові методи передачі даних. Рішення цієї проблеми - мережа нового покоління (NGN). NGN (англ. The Next Generation Network) – це мультисервісна мережа, ядром якої є мережа IP, яка підтримує повну або часткову інтеграцію мови, даних та мультимедійних послуг. Реалізує принцип конвергенції телекомунікаційних послуг.

Спочатку були побудовані окремі мережі зв'язку для передачі різних типів інформації: телефонна мережа, телеграфна мережа, мережа передачі даних тощо. У другій половині XX століття з'явилася ідея об'єднати всі мережі зв'язку в одну. Так було створено концепцію мереж ISDN. Об’єднувальною мережею мережі ISDN є Телефонна Мережа Загального Користування.

Але наприкінці XX століття через різні причини (висока вартість обладнання ISDN, швидкий розвиток IP-мереж, поява нових додатків та служб) ідея формування глобальної мережі ISDN провалилася. Концепція мереж ISDN була замінена концепцією мереж NGN нового покоління. На відміну від мережі ISDN, мережа NGN спирається на мережу даних на основі IP.

За своїм найпростішим визначенням, мережа NGN - це відкрита, стандартна пакетна інфраструктура, яка може ефективно підтримувати всю гаму існуючих додатків та служб, забезпечуючи необхідну масштабованість та гнучкість для відповіді на нові вимоги щодо функціональності та пропускної здатності.

Розвиток ринку послуг зв'язку привело до наступних передумов появи мереж NGN:

- масовому впровадженню сучасних систем і засобів зв'язку, характерні риси - мультисервісність і мультипротокольність;
- істотної зміни мережевих архітектур: відмови від жорсткої ієрархії, характерною для класичних телефонних мереж загального користування (ТМЗК), під впливом впровадження нових засобів зв'язку, принципів передачі та обробки інформації;
- функціональному поділу рівня транспортної комутованої мережі і рівня формування послуг, виник в результаті впровадження інтелектуальних мереж (IN) і закріпленому в NGN (завдяки Інтернету, оператору не обов'язково мати власну транспортну мережу, а спектр послуг вийшов за рамки традиційних послуг зв'язку;)
- загострення конкуренції в динамічних секторах ринку, таких як мобільний зв'язок, Інтернет, послуги для корпоративних користувачів;
- поділу бізнес-моделі оператора нових послуг на дві частини: інфраструктурну (створення і обслуговування мережі) і сервісну (пов'язану з маркетингом);
- наявності проміжних ланок - віртуальних операторів формує і реалізують пакети послуг з доданою вартістю, як це роблять системні інтегратори в IT;
- зміни статусу інфокомунікаційних послуг: власне мережу втрачає свою цінність, її набувають послуги;
- зменшення ролі / частки голосових послуг в сучасних пакетах Triple Play (TP) і Quadruple Play (QP)
- використання умовно безкоштовних послуг, заснованих на експлуатації мережі Інтернет (наприклад, послуга, що надається по Skype)
- зниження інвестиційної привабливості, конкурентоспроможності та рентабельності традиційних систем зв'язку.

1.1. Аналіз побудови телекомунікаційних мереж на базі концепції NGN.

Багаторівнева архітектура NGN.

Особливість концепції мереж NGN від традиційних мереж полягає в тому, що вся інформація, що циркулює в мережі, розділена на два компоненти. Це сигнальна інформація, яка забезпечує перемикання абонентів та надання послуг, а також дані користувача, що містять корисні навантаження, призначені абоненту (голос, відео, дані). Шляхи сигнальних повідомлень та корисне навантаження користувача може не збігатися.

Мережі NGN на базі Інтернет-технологій включають протокол IP та MPLS. На сьогодні розроблено кілька підходів до побудови мереж IP-телефонії, запропонованих організаціями MCE-T та IETF: H. 323, SIP та MGCP.

В більшості публікацій з NGN принципів побудови мереж наступного покоління наводиться узагальнена 4-х рівнева архітектура NGN, в якій виділяються такі рівні (рис. 1.1).

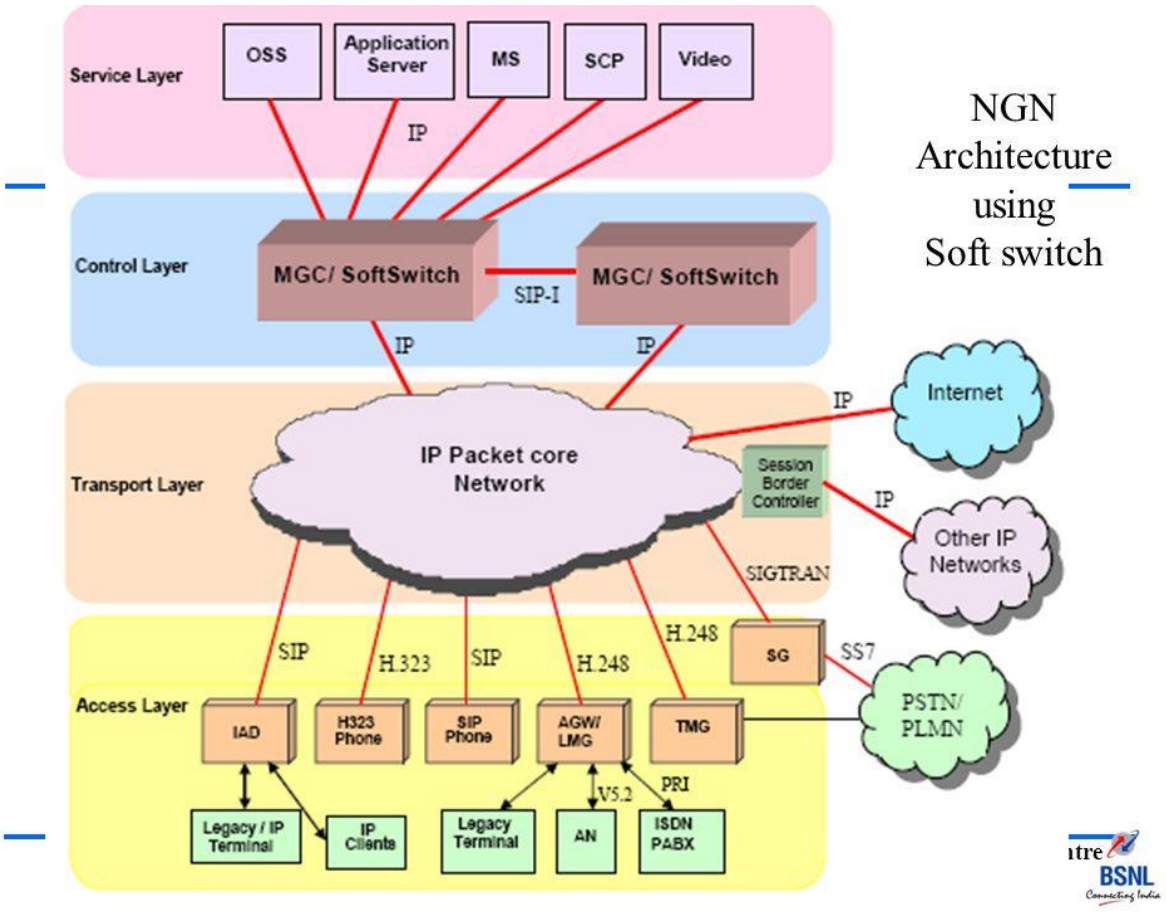

РИС. 1.1. Узагальнена 4-х рівнева архітектура NGN

● рівень доступу, що містить мережу доступу абонента до транспортної пакетної мережі;

● транспортний рівень, який включає мережу пакетної магістралі (мережа, побудована на основі протоколів комутації пакетів IP або ATM, в даний час найчастіше базується на технології MPLS та протоколі IP);

● комутаційний рівень управління, який включає набір функцій для управління всіма процесами обслуговування дзвінків у телекомунікаційній мережі;

● рівень обслуговування та оперативного управління, який містить логіку виконання служб та / або додатків та керує цими службами, має відкриті інтерфейси для використання сторонніми організаціями (для розробки програм та нових сервісів).

Термінальне обладнання не є частиною мережі NGN і може в принципі бути будь-яким із наборів абонентського обладнання існуючих дротових та бездротових мереж. Однак таке кінцеве обладнання може бути підключено до мережі NGN лише через відповідний шлюз абонентського обладнання рівня доступу. Пряме підключення до мережі можливе лише для пакетних абонентських терміналів, які використовують протоколи SIP та H. 323.

Слід зазначити, що в деяких публікаціях зустрічається ще простіша 3-х рівнева архітектура NGN, в якій функції рівня доступу і транспортної мережі об'єднані в один транспортний рівень.

Технології використання на кожному рівні.

Яким би не був шлях створення NGN, присутність елемента, що відповідає за управління процесом встановлення з'єднання, неминуче. Мова йде про класичну зв'язку між двома системами: керуючої і керованої (рис. 1.2.).

РИС. 1.2. Керуюча і керована система

Довгий час єдиним кандидатом на роль керуючої системи був сигнальний комутатор Softswitch. З часом у нього з'явилися конкуренти, основним з яких виступає IMS. А для об'єднання різних IP-мереж і доменів необхідний граничний контролер сесій - SBC (Session Border Controller).

Функції і архітектура Softswitch

Термін "Softswitch" використовується не тільки для ідентифікації одного з мережевих елементів. З нею пов'язана архітектура мережі і навіть, певною мірою, сама ідеологія побудови мережі. Для нас важливими є функції, які виконує перемикач Softswitch та його здатність вирішувати ряд завдань, притаманних вузлам з перемиканням каналів.

Перш за все, перемикач Softswitch керує обслуговуванням дзвінків, тобто встановленням та припиненням з'єднань. Так само, як це стосується традиційних систем банкоматів з комутованою схемою, якщо встановлено з'єднання, ці

функції гарантують, що він залишатиметься встановленою ймовірністю, поки абонент, абонент або абонент, який викликається абонентом, не буде відключений. У цьому сенсі перемикач Softswitch можна розглядати як систему управління.

Функції управління послугами дзвінків включають в себе розпізнавання та обробку номерів для визначення місця призначення, а також розпізнавання моменту відповіді, моменту, коли один з абонентів зависне, та реєстрації цих дій для стягнення плати. Таким чином, Softswitch фактично залишається тим самим звичним вузлом комутації, тільки без цифрового поля комутації та наборів абонентів, що дозволяє легко інтерпретувати його функції в різних сценаріях модернізації мережі загального телефонного зв’язку (PSTN). Відповідальність за вищезазначені операції Softswitch покладається на функціональний елемент, що входить до його агента виклику.

Інший термін, часто асоційований із Softswitch, - це контролер транспортного шлюзу MGC. Ця назва підкреслює той факт, що транспортом та шлюзами доступу керують за допомогою протоколу H. 248 або подібного. Softswitch координує обмін сигнальними повідомленнями між мережами, тобто підтримує функціональність шлюзового сигналу (SG). Він координує дії, які забезпечують з'єднання з об'єктами в різних мережах, і вносить інформацію в повідомлення. Така трансформація необхідна для того, щоб сигнальні повідомлення трактувалися однаково по обидва боки різних мереж, забезпечуючи роботу автоматичних телефонних станцій (АТС) з першого етапу модернізації.

На рис. 1.3 показано місце Softswitch і його взаємодію з різними існуючими і перспективними елементами мереж загального користування по відповідних протоколах.

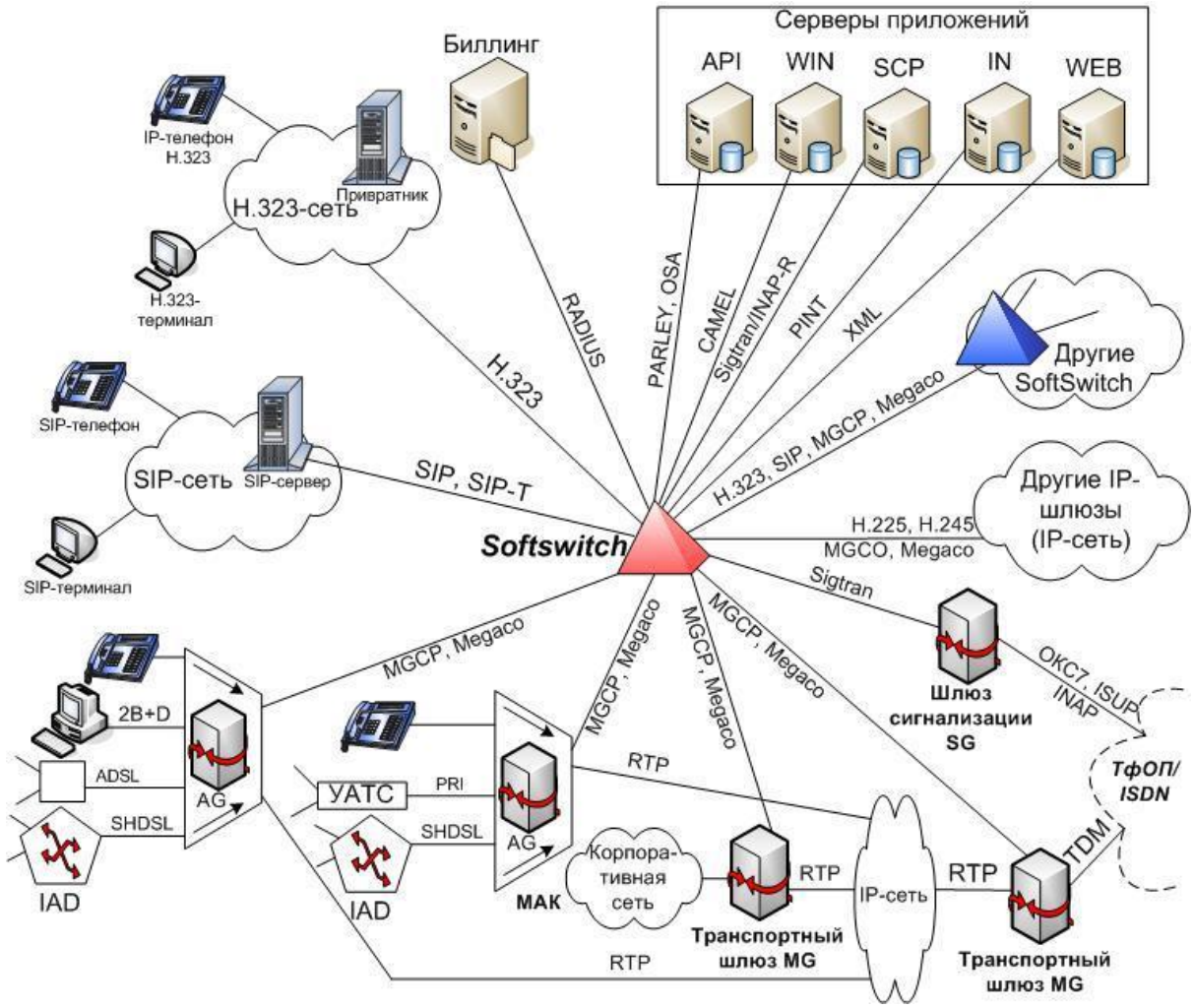

РИС. 1.3. Softswitch в скаладі ЄСЕ.

З точки зору сценаріїв модернізації ТМЗК і ЄСЕ в цілому нас також цікавить архітектура побудови Softswitch і поділ цього обладнання на 4-й і 5-й класи. Історично склалося, що поділ на класи автоматично було перенесено на Softswitch, однак насправді це заслуговує на увагу лише в разі впровадження Softswitch замість вузла з комутацією каналів. З точки зору передачі мови по IP-мережі (Voice over IP, VoIP) цей поділ буде не зовсім коректним. При роботі будь-якого сигнального протоколу VoIP немає відмінностей, наприклад, між SIP-телефоном і Proxy-сервером SIP. Тому поділ на транзитні і місцеві пристрої для Softswitch важливо лише при роботі в ТМЗК.

Еталонна архітектура мереж на базі Softswitch, складається з чотирьох умовних функціональних рівнів (рис. 1.4.).

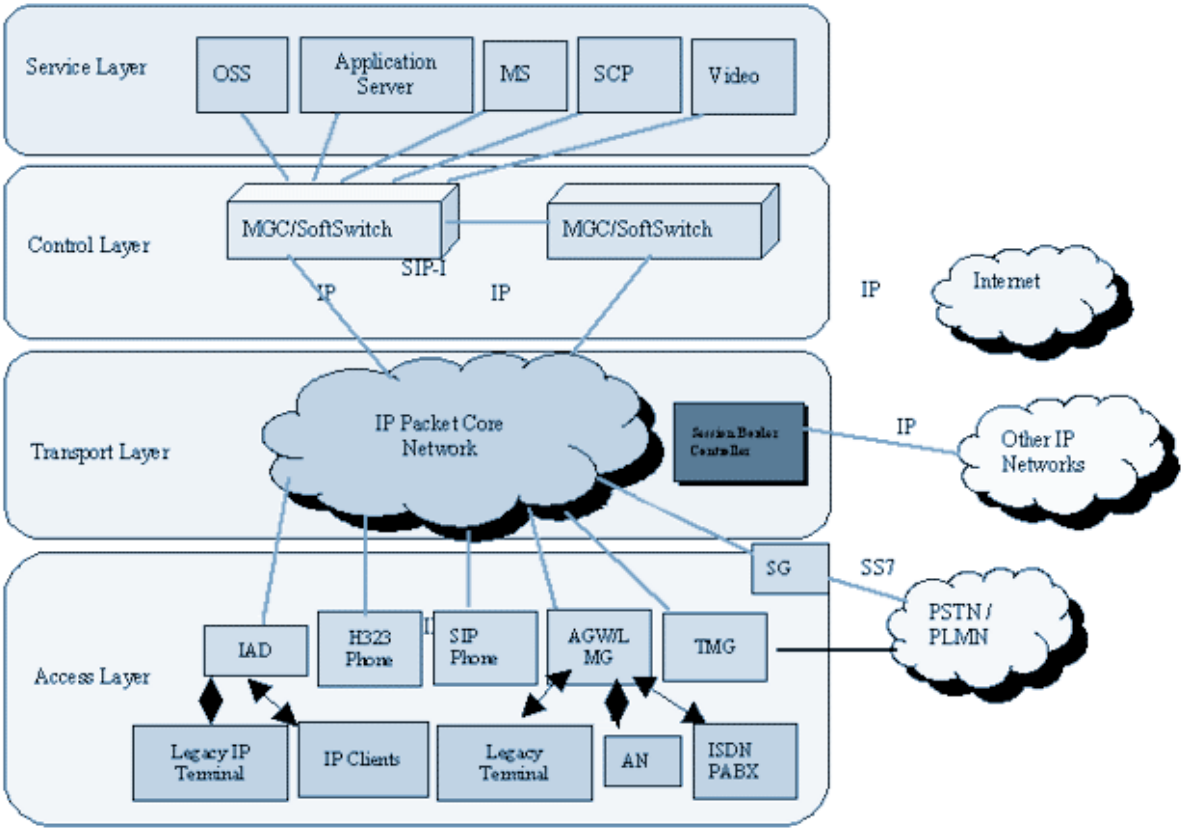

РИС. 1.4. Еталонна архітектура мереж на базі Softswitch.

Внизу архітектури знаходиться транспортний рівень (Transport Layer), який відповідає за перенесення по VoIP-мережі сигнальних повідомлень та мультимедійної інформації.

Рівень управління викликами і сигналізації (Call Control & Signaling) управляє основними елементами VoIP-мережі, особливо що знаходяться на транспортному рівні. На цьому рівні знаходяться такі пристрої, як контролери медіа-шлюзів (MGC, Call Agent, Call Controller).

Рівень послуг і додатків (Service & Application) забезпечує управління, логіку і виконання деякого числа послуг або додатків.

Рівень управління (Management & Access) виконує функції користувальницького забезпечення, підтримки операцій і надання послуг, а також вирішує завдання білінгу та інші завдання мережевого управління. Рівень управління може взаємодіяти з будь-яким з трьох перерахованих рівнів, використовуючи стандартні або внутрішньо фірмові протоколи і програмні інтерфейси API.

У центрі кожного з таких рішень знаходиться сам Softswitch, який теоретично відноситься до рівня управління викликами і сигналізації, але в практичних рішеннях в тій чи іншій мірі захоплює функції інших рівнів архітектури.

Таким чином, при фактичному дотриманні принципу функціональної декомпозиції шлюзу можна спостерігати різні варіанти його реалізації. Перші Softswitch-рішення представляли собою єдиний блок, тобто фізичної декомпозиції шлюзу не було, але існував розподіл функцій програмних або

апаратних модулів. Іншими словами, обладнання мало інтегровану архітектуру. В іншому варіанті фізично відокремлювався лише медіа-шлюз, а контролер медіа-шлюзів і шлюз сигналізації становили єдиний комплекс. Таке рішення можна вважати частковою фізичної декомпозицией.

Разом з тим при всіх перевагах в Softswitch залишалося кілька проблем, без вирішення яких подальший розвиток цієї технології суттєво ускладнювався. Основними з них стала реалізація функції системи оперативно-розшукових заходів (СОРМ), відстеження показників QoS (особливо в разі укладення угод про рівень обслуговування SLA - Service Level Agreement) і подолання міжмережевих екранів. Поява контролерів SBC стало вирішенням цих проблем.

Використання контролерів SBC

Основне завдання SBC - інтерактивне з'єднання окремих IP-мереж. Більшою мірою їх переваги проявляються при передачі через кордони мереж голосового, відео- або мультимедійного трафіку, тобто трафіку реального часу.

Традиційно провайдери IP-телефонії взаємодіяли між собою, використовуючи голосові шлюзи (Media Gateway), підключені до телефонних комутаторів. Така схема роботи дозволяє забезпечити безпеку з'єднання і надати всю необхідну білінгову інформацію. Правда, за рахунок додаткового перетворення в кодеках знижується якість голосу і підвищується вартість пропуску трафіку. До того ж така схема не дає можливості пропускати трафік інших мультимедійних додатків (таких, як Instant Messaging і відеопотоки). Але поки трафіку IP-телефонії в світі було мало і він в основному носив характер з'єднань типу "точка - точка", це не викликало великих проблем.

Для вирішення проблеми міжоператорської взаємодії і був створений SBC, після чого замість схеми "IP-TDM-IP" стало використовуватися пряме з'єднання "IP-IP". Крім того, SBC бере на себе забезпечення взаємодії мереж:

- міжпротокольних (двостороння трансляція сигнальних протоколів SIP і H.323);
- внутрішньо протокольних (перетворення різних версій стеків протоколів);
- міжоператорських;
- міжвендорних (включаючи передачу факсів по протоколу T.38);
- контроль за встановленням телефонних з'єднань (Call Admission Control, CAC);
- регулювання якості голосу шляхом обмеження числа одночасно активних викликів;
- безпечність (включаючи функції RTP proxy для приховування внутрішньої структури мережі);
- можливість роботи через пристрій перетворення мережевих адрес NAT (Network Address Translation) і міжмережеві екрани (забезпечення проходження трафіку);
- забезпечення СОРМ.

Це означає, що контроллер SBC встановлюється на границях мережі і виконує ті функції, які не доцільно покладати на Softswitch. У цьому ідея

застосування контролерів SBC нагадує введення периферійних пристроїв управління для поліпшення роботи першого покоління АТС з програмним управлінням, в яких функції управління були реалізовані в двомашиному комплексі спеціалізованих ЕОМ. Також треба розуміти, що SBC працює з такими мережевими пристроями, як Softswitch, міжмережевий екран (Firewall), пристрій перетворення мережевих адрес NAT, але не замінює їх.

Функціональність SBC значно ширше, ніж це необхідно "помічнику" Softswitch. Слід зазначити, що поділ функціональності між системами Softswitch і SBC дуже розмиті. Softswitch може брати на себе більшість функцій SBC, залишаючи останньому лише функцію нормалізації трафіку, тобто узгодження кодеків, DTMF (багаточастотний набір) та ін. Завдання Softswitch фокусуються на управлінні медіа-шлюзами і маршрутизації викликів між ТМЗК та IP-мережею або всередині IP -мережі. SBC з самого початку орієнтований на набагато більшу кількість послуг реального часу (відео, мультимедіа, Instant Messaging), що реалізуються в IP-мережі. Трафіку, який пропускають через SBC, забезпечується управлінням якістю обслуговування, безпекою, пропускною здатністю, але SBC не виконує функції маршрутизації. Тому для взаємодії мереж необхідно одночасне використання обох видів обладнання - Softswitch і SBC.

Продукти SBC можуть мати розподілену архітектуру. Вона включає в себе центральний вузол CSBC (Core SBC), що знаходиться в межах мережі провайдера, і кінцеві пристрої ESBC (Edge SBC), які встановлюються на кордоні мережі. При цьому CSBC розподіляє трафік між ESBC.

За логікою SBC можна розділити на два функціональні модулі, один з яких стосується всього, що стосується сигналізації (SBC-SIG), а інший працює з трафіком користувачів (SBC-MEDIA). На ринку є два варіанти будівництва SBC:

- інтегрований, в якому обидва функціональних модуля розташовані в складі єдиного апаратного комплексу;
- розподілений, коли кожен з модулів знаходиться в різних мережевих елементах, що взаємодіють по протоколу H.248 або COPS-PR.

Інтегровані рішення SBC представляють зазвичай двопортові пристрої: один з портів звернений до зовнішньої мережі, а другий - до внутрішньої. У цьому випадку кожен порт використовується як для даних, так і для сигналізації, що створює ризик втрати сигнальних пакетів.

У разі розподіленої архітектури SBC-SIG розташовується в мережі провайдера, а модулі SBC-MEDIA виносяться на границі мережі. Весь сигнальний VoIP-трафік з зовнішніх мереж направляється до SBC-SIG. При цьому центральний пристрій SBC-SIG може обробляти сигналізацію, що надходить з декількох точок доступу, і управляти знаходжуваних в них SBC-MEDIA. Крім того, функція SBC-SIG може бути реалізована в комутаторі Softswitch, керуючому мережею провайдера, що найчастіше вже має місце в існуючих Softswitch-рішеннях.

Якщо не розбирати детально кожну функцію SBC, а замість цього поставити наступне питанням: чи потрібен Softswitch при використанні SBC? Можна застосувати схему, що складається з Softswitch і SBC-media на кордонах

мережі. А можна використовувати розподілену архітектуру SBC, і обійтися без Softswitch. Адже розширення функціональності SBC може практично порівняти його з найпростішими Softswitch-рішеннями 4-го класу.

Можливо, це і стало б черговою проблемою в концепції NGN. І ми отримали б два різних рішення, але, на щастя, знайшлися два аргументи на користь застосування Softswitch. По-перше, взаємодія з пристроями ТМЗК явно виходить за рамки функціональності SBC. По-друге, поява нового окремого пристрою в мережі навряд чи доцільно: простіше доопрацювати Softswitch модулем SBC-SIG. Правда, треба відзначити, що Softswitch може обслуговувати кінцеве число викликів в одиницю часу. У цьому плані застосування SBC має важливе значення, оскільки характеризується кращими показниками по масштабованості. З цих міркувань симбіоз Softswitch і SBC є досить вдалим союзом.

Після того, як ідея передачі голосу через комутаційні мережі та протокол IP була успішною, оператори серйозно задумалися про зміну існуючих телекомунікаційних мереж. За розвиток взаємозв'язку телекомунікаційних мереж із технологіями пакетної комутації взялася група 3GPP. Поява пакетного доступу в стільникових мережах вважається 99-м випуском 3GPP (3GPP R99), який запровадив підтримку домену PS у існуючих мобільних мережах на основі технології GPRS. Але робота тривала в 4-му випуску, абоненти комутації лежали на програмному перемикачі SoftSwitch (R4 3GPP). П'ятий випуск (R5 3GPP) ознаменував появу архітектури IMS, хоча спочатку лише як підсистему надання мультимедійних послуг, але пізніше (3GPP R5) архітектура стала ключовою і переключила користувачів на себе.

1.2. Недоліки NGN.

Більшість фахівців, які обговорюють проблеми впровадження мереж NGN на ринок зв'язку, на перше місце ставлять проблему відсутності нормативної бази. Також при впровадженні NGN повинні бути вирішені проблеми сумісності обладнання з існуючими телекомунікаційними мережами. Особливе значення надають проблемі взаємодії з СОРМ.

Ще однією проблемою вважається відносно високий рівень початкових вкладень, перш за все на проектування IP - мережі. Операторам в регіонах будувати мережу NGN дещо простіше, так як регіональні, наземних ліній не настільки великі, замінити застаріле обладнання істотно простіше, ніж в великих містах, де регулярно відбувається модернізація мережі ТМЗК.

Іншим фактором, який ускладнює впровадження NGN, є інертність людської поведінки. У Європі телефонні апарати орендуються користувачами і якщо на ринку з'являється новий апарат, користувач практично безкоштовно може обміняти свій телефон на новий. В Україні ж користувачі купують той чи інший засіб зв'язку виходячи з власних переваг і можливостей. Як наслідок, частина нових послуг встигає застаріти, залишившись непотрібними для цілого ряду абонентів. А ефективне використання технології NGN передбачає, що у

користувача повинна бути IP-телефонія, як первинна ланка NGN, але не схема телефон - телефон, як зараз, а комп'ютер - комп'ютер.

Також певну складність являє собою регулярна поява стандартів на обмін даними, більшість компаній не можуть дозволити собі бути залежними від інформаційних технологій, тому частина з них встигає застаріти ще до масової апробації.

Ще однією вимогою при впровадженні мережі є такий фактор, як коефіцієнт готовності. IP телефонія знаходиться в повній залежності від струму в мережі, по порівняння зі стандартними телефонами, підключеними до ТМЗК, які не припиняють працювати навіть при відключенні електрики. З цієї причини частина операторів не ризикують переходити на програмний комутатор, в тому числі тому, що до АТС підключені не тільки абоненти, а й служби екстреного реагування.

Крім цього, для чисто голосової телефонії NGN неефективна. Звичайний маршрутизатор, без проблем обслуговуючий 10 комп'ютерів, буде мало ефективний для обслуговування 10 телефонів, тому що телефонія працює в реальному часі і у неї інші вимоги до продуктивності.

1.3. Шляхи усунення недоліків - перехід до концепції IMS

Виробники, як правило, роблять акцент на кількох ключових відмінностях IMS від попередніх конвергентних рішень. Для початку фахівці відзначають, що основна перевага і відмінність концепції IMS від інших технологій NGN полягає в можливості мульти-стандартного доступу до послуг, коли одні й ті ж послуги можна отримувати за допомогою різних мереж доступу -від широкосмугового xDSL до Wi-Fi або UMTS. При цьому зміна мереж доступу відбувається непомітно.

На рівні обслуговування і SS, і IMS можуть відокремлювати управління викликами від службових програм і мати важливу функцію забезпечення відкритих інтерфейсів служб.

SS пропонує нові додаткові послуги через інтерфейс прикладного програмування (API) і сервер додатків. Крім того, надання базових послуг виклику і додаткових послуг ТМЗК логічно інтегровано в SS. За допомогою протоколу інтелектуальних мережевих додатків (INAP) SS може працювати з існуючою точкою управління службами (SCP) в інтелектуальній мережі (IN) для надання традиційних послуг IN. Для підтримки інтелектуальних послуг ТМЗК SS може бути підключений до регістру визначення місця розташування «розумного домашнього реєстру» (SHLR) через інтерфейс протоколу мобільних додатків (MAP) для реалізації централізованого управління даними обслуговування користувачів.

Архітектура IMS визначає інтерфейс IMS Service Control (ISC) в якості контрольної точки управління службами для з'єднання з сервером додатків на основі SIP. Інтерфейс ISC дозволяє сервісним додаткам бути індивідуальними або комбінованими, а також забезпечує взаємодію між різними серверами сервісних додатків. Відповідно, це забезпечує сумісність всієї мережі і сервісних терміналів. Сама IMS не інтегрує ніякої сервісної логіки. Логіки послуг ТМЗК

заповнюються незалежними серверами додатків PES / PSS (APP) через інтерфейс ISC. Більш того, сама IMS не керує ніякими даними користувачів. Для реалізації уніфікованого управління профілями користувачів і службовими даними всі призначені для користувача дані підключаються до домашнього абонентського сервера (HSS), який ще називається TISPAN функцією сервера профілів користувачів (UPSF) через інтерфейс Diameter.

На рівні управління SS використовує один функціональний об'єкт для виконання таких функцій, як обробка та управління викликами, адаптація протоколу доступу, надання інтерфейсу служби, функціональна сумісність і взаємодію, управління даними користувача і логіка обслуговування PSTN. Однак IMS виконує згадані функції більш незалежними функціональними об'єктами, включаючи функцію управління сеансом виклику (CSCF), функцію управління медіа-шлюзом (MGCF), функцію управління шлюзом доступу (AGCF), функцію управління медіаресурсами (MRCF) і управління шлюзом комутації Функція (BGCF) . Основна функція CSCF додатково ділиться на Проксі-CSCF (PCSCF), яка обслуговує CSCF (SCSCF) і яка запитує CSCF (ICSCF). PCSCF є першою контактною точкою для призначеного користувача терміналу в IMS. SCSCF фактично управляє станами сеансу в мережі. ICSCF є точкою контакту в мережі оператора для всіх з'єднань IMS, призначених для абонента цього оператора мережі або роумінгового абонента, в даний час знаходиться в зоні обслуговування цього оператора мережі.

На рівні доступу SS і IMS можуть підтримувати поділ доступу і контролю. Їх пристрої доступу дуже схожі і можуть навіть взаємодіяти один з одним. Магістральний шлюз / сигнальний шлюз H.248 (TG / SG) і призначений для користувача шлюз доступу (AG) в SS можуть бути таким самим медіашлюзом / сигнальним шлюзом (MGW / SGW) і шлюзом доступу (AGW) в IMS. Крім того, комунікаційний сервер і процесор функцій медіаресурсу (MRFP) виконують в основному одну і ту ж функцію. У IMS існують стандарти доступу до мобільних SIP-терміналів, тоді як стандарти доступу абонентів PSTN все ще вдосконалюються.

На рівні каналу IMS пропонує повноцінну архітектуру all-IP. Щоб використовувати QoS, IMS використовує підсистему підключення до мережі (NASS) і підсистему управління ресурсами та доступом (RACS), яку називають функцією визначення політики (PDF). Однак SS робить упор на архітектуру IP базової мережі, щоб забезпечити перехід від існуючої мережі до мережі allIP; таким чином, гарантія QoS залежить від самої IP-мережі.

Споживачеві перехід на IMS обіцяє появу персоналізованих послуг, заснованих на передачі мови, тексту, графіки і відео в будь-якій комбінації, створення нових сервісів, а також об'єднання та вдосконалення існуючих. IMS відкриває дорогу послуг Push-to-Talk (напівдуплексний зв'язок, коли стільниковий телефон використовується як термінал системи професійної мобільного радіозв'язку) з функцією визначення присутності абонента, технології UMA (Unlicensed Mobile Access), PhotoTalk , Instant Messaging, MultiChat і багатьом іншим.

1.4. Історія розвитку IMS

IMS, відома як IP Multimedia Subsystem, являє собою базову мережу IP-мультимедіа і телефонії, яка визначається стандартами 3GPP і 3GPP2 і організаціями на основі інтернет-протоколів IETF. IMS - це набір специфікацій, які описують архітектуру мереж наступного покоління (NGN) для реалізації послуг телефонії та мультимедіа на основі IP. Він визначає повну архітектуру і структуру, яка дозволяє інтегрувати технології передачі голосу, відео, даних і мобільних мереж в інфраструктуру на основі IP.

IMS не залежить від доступу, оскільки підтримує IP-сеанси по провідній IP-мережі, 802.11, 802.15, CDMA, пакетним даними, а також GSM / EDGE / UMTS і іншим додаткам пакетної передачі даних. Перш ніж перейти до деталей, давайте поглянемо на історію IMS.

Спочатку IMS була визначена галузевим форумом під назвою 3G.IP, створеним в 1999 році. 3G.IP розробив первинну архітектуру IMS, яка була представлена в рамках проекту партнерства 3-го покоління. Вперше він з'явився у випуску 5, коли був доданий мультимедійний контент на основі SIP. 3GPP2 заснував свій мультимедійний домен CDMA2000 на IMS 3GPP, додавши підтримку CDMA2000. В 3GPP версії 6 додана підтримка взаємодії з WLAN. У версії 7 3GPP додана підтримка фіксованих мереж завдяки спільній роботі з версією TISPAN R1.1.

1.5 Висновки до розділу.

У пунктах даного розділу розглядається інформація про те як архітектура IMS виникла в результаті еволюційного процесу NGN.

З точки зору базової архітектури мережі і цілі, SS і IMS повністю ідентичні. Вони обидві засновані на IP-мережі. Крім того, обидві вони роблять акцент на поділі управління викликами і каналами обслуговування, а також на відкритій платформі обслуговування. З точки зору технічних тенденцій, IMS підтримує мобільність і мультимедійні послуги, має високий ступінь відкритості та конвергенції. IMS являє майбутню тенденцію розвитку конвергенції , отже, являється більш перспективною концепцією, можна сказати, що мережа на основі SS є основною стадією розвитку NGN, а мережа на основі IMS є розширеною стадією NGN. Тому для постачальників і операторів обладнання важливо розвивати мережу за допомогою SS в повноцінну архітектуру IMS.

Розділ 2. Концепція мультимедійної підсистеми IMS.

2.1. Принцип побудови IP Multimedia Subsystem

Надання привабливих для абонентів послуг нового покоління вимагає зміни принципів побудови мереж. Ще не так давно доставка телекомунікаційних послуг була орієнтована на абонентське обладнання. З розширенням спектра послуг були потрібні нові пристрої (наприклад, модеми), а реалізація послуг

здійснювалася по вертикальній схемі, тобто для кожної послуги необхідна була окрема інфраструктура. Зараз, коли можна звертатися в кілька мереж і використовувати різні комунікаційні пристрої, в тому числі мобільні, практика надання послуг о вертикальній схемі викликає незручності.

Вирішальним фактором для розвитку телекомунікаційних технологій є не тільки потреби корпоративного сектора. Перш за все, це традиційно великі витрати на зв'язок. У сегменті індивідуальних абонентів, попит зростає на послуги широкосмугового доступу з можливістю доставки відео, участі в онлайнових іграх і використання інших сучасних додатків.

Щоб утримати клієнтів, оператори змушені вдосконалювати набори послуг. Крім того, їм доводиться враховувати зростаючий тиск конкурентів, які також виводять на ринок привабливі сервіси.

Єдина комунікаційна інфраструктура на основі IP - оптимальне рішення цієї проблеми. Вона використовується для організації всіх типів послуг і здатна взаємодіяти з різними термінальними пристроями. Наявність універсальної технологічної середовища забезпечує інтеграцію різних комунікаційних додатків. Таке середовище повинно підтримувати здійснення персональних комунікацій в реальному масштабі часу (наприклад, сеанси голосового зв'язку) в пакетній мережі, не вдаючись до технологій, орієнтованим на комутацію каналів. Разом з тим, це середовище має забезпечувати взаємодію з зовнішніми мережами традиційної телефонії як для фіксованої, так і для мобільного зв'язку. Для реалізації такого середовища була запропонована архітектура IP Multimedia Subsystem (IMS - мультимедійна підсистема з IP).

Концепція IMS була запропонована на форумі 3GPP. 3GPP - проект координації розробки рішень для мереж третього покоління. Ця концепція визначає мережеву архітектуру, яка спирається на пакетну транспортну мережу і забезпечує підтримку різних варіантів доступу. Архітектура, в свою чергу, передбачає взаємозв'язок ряду функціональних елементів. Функціональні елементи зв'язуються один з одним за допомогою інтерфейсів. У кожного такого інтерфейсу є своя назва, за яким ховається певний протокол.

Архітектура IMS розроблялася для використання в мережах рухомого зв'язку третього покоління. Підтримка протоколу ініціювання сеансів зв'язку (SIP) дозволяє використовувати єдиний підхід до реалізації програм і здійснення доступу, а також інтегрувати програми, пропоновані сторонніми компаніями (наприклад, контент-провайдерами).

У релізах 6 і 7 (так називаються документи 3GPP) визначена ідеологія здійснення IP-комунікацій за допомогою SIP. Відповідно до неї, SIP починається безпосередньо з мобільного терміналу.

В архітектурі IMS визначено кілька функціональних елементів. Наприклад, замість традиційних для мобільних мереж комутаторів MSC використовуються проксирующі елементи, які називаються Proxy-Call Session Control Function. Як і в GSM, в IMS є інтерфейсні точки, або ж інтерфейси, які пов'язують ці функціональні елементи один з одним. У кожного інтерфейсу є своя назва, і за ним стоїть певний протокол. Найпростіший приклад - інтерфейсна точка ISC, яка пов'язує сервісний проксі з сервером додатків на основі протоколу SIP.

Концепція створення архітектури IMS виявилася настільки вдалою, що деякі органи стандартизації запропонували використовувати її для мультисервісних рішень в своїх секторах ринку. Організація CableLabs, що розробляє стандарти для мереж кабельних операторів, в специфікації Fast Cable 2.0 передбачає впровадження SIP. І всюди в основі лежить ідея IMS.

Це цілком логічно, оскільки протокол IP визнаний в якості основи для мереж нового покоління, а SIP - як інфраструктурного протоколу для доставки додатків. Інтенсивний розвиток великого числа додатків, що використовують SIP, обумовлює необхідність побудови масштабованої мультисервісної інфраструктури, яка б розділяла транспортний рівень, рівень послуг і рівень управління. Така сервісна "прошарок" приховує від абонента різницю між послугами, які надаються, наприклад, в мережі бездротового доступу, і послугами, які надаються в мережі кабельного телебачення або використовують мережі доступу на основі DSL, а також Ethernet.

У концепцію IMS дійсно закладений принцип, відповідно до якого ця архітектура має можливість для встановлення великого числа сеансів зв'язку, причому беруть участь в цих сеансах абоненти які можуть використовувати різні пристрої доступу. Абонентам пропонуються різного роду послуги, доставка яких ґрунтується на загальному підході.

Зокрема, така архітектура має можливість для вирішення таких завдань, як реалізація декількох послуг в рамках одного сеансу зв'язку. При цьому у обслуговуючого абонента не повинно виникати проблем з різними видами термінального обладнання. Зокрема, має гарантуватися встановлення сеансу зв'язку в разі, коли використовуваний термінал не володіє певними функціональними можливостями. Це означає, що при відеотелефонії виклику передбачається можливість його прийому без відеокомпонентів, або ж відео перенаправлятиметься на інший пристрій.

Послуги в процесі одночасного надання повинні розділятися на ті, які вимагають синхронізації (наприклад, синхронізація відео і голосу в відеотелефонії), і на ті, які не вимагають синхронізації (наприклад, відео та чат).

2.2. Функціональні компоненти, функціональні площини IMS

IMS поділяє мережеву інфраструктуру на окремі функції з стандартизованими інтерфейсами між ними. Кожен інтерфейс називаються як «точка відліку», який визначає протокол, між яким він працює. На наступному малюнку показаний огляд архітектури IMS:

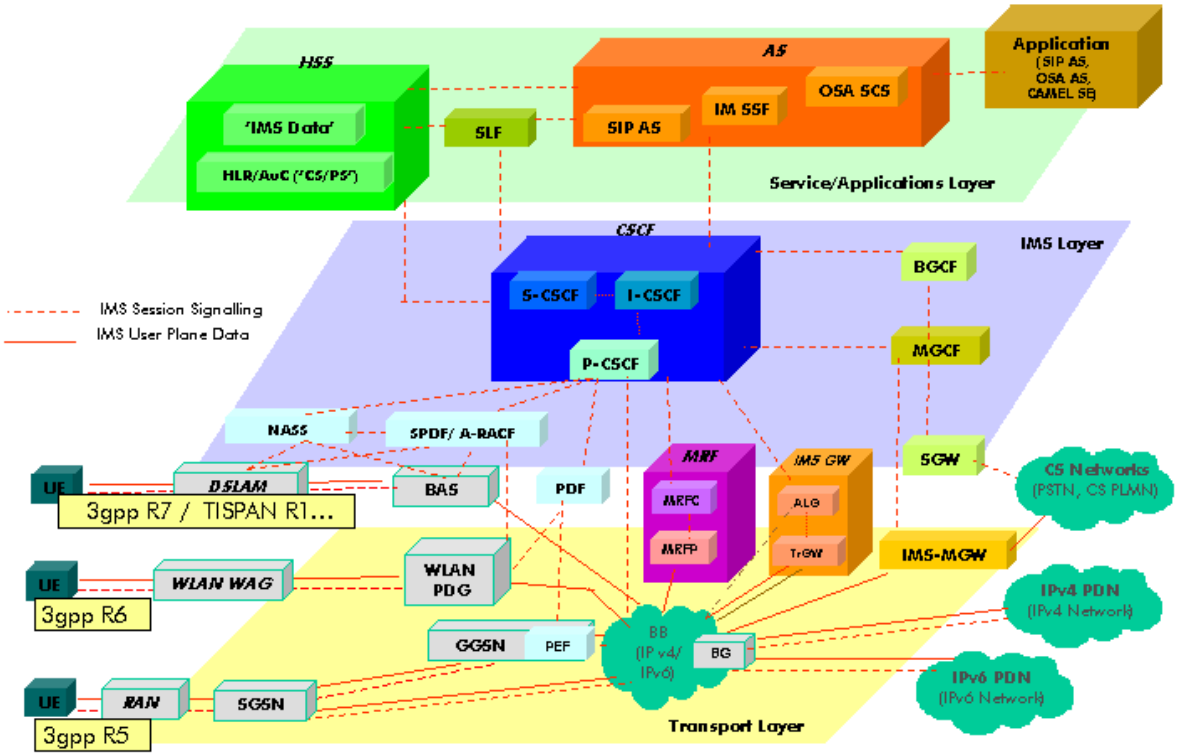

РИС. 2.1. Загальна архітектура IMS

Як показано на рис.2.1, архітектура розділена на три основні рівні, кожен з яких описується рядом еквівалентних імен:

- Транспортний рівень
- Рівень управління сеансом
- Рівень сервера додатків

1. Транспортний рівень.

Цей рівень залучений в ініціювання та завершення сигналізації SIP, настройку сеансів і надання послуг каналу-носія. Цей рівень також надає медіашлюзи для перетворення даних VoIP в формат TDM PSTN.

2. Рівень управління сеансом.

Цей рівень містить функцію управління сеансом виклику (CSCF), до функцій якої входить надання кінцевих точок для реєстрації і маршрутизації повідомлень сигналізації SIP, що дозволяє направляти їх на відповідні сервери додатків. CSCF гарантує QoS, зв'язуючись з транспортним і кінцевим рівнями.
Типи CSCF:

- Проксі-CSCF (P-CSCF) - це SIP-проксі, який є першою точкою контакту для терміналу IMS. Призначається терміналу IMS при реєстрації і не змінюється протягом терміну реєстрації. Створює записи про оплату

- Обслуговуючий CSCF (S-CSCF) є центральним вузлом площині сигналізації. Це SIP-сервер, який також виконує управління сеансом. Він використовує інтерфейси Diameter Cx і Dx для HSS для завантаження і завантаження призначених для користувача профілів - у нього немає локального сховища користувача. Вся необхідна інформація завантажується з УСЗ. Обробляє реєстрації SIP, що дозволяє прив'язати розташування користувача і адресу SIP. Вирішує сервери додатків призначення, на які буде пересилатися повідомлення SIP, для надання послуг. Надає послуги маршрутизації, використовуючи пошук по електронній нумерації. Забезпечує дотримання політики оператора мережі. Кілька S-CSCF співіснують в одній мережі для забезпечення розподілу навантаження і високої доступності. Але HSS, призначає S-CSCF користувачеві, коли його запитує I-CSCF.
- I-CSCF (Interrogating-CSCF) є проксі-сервером SIP, який забезпечує функцію пошуку служби. Його основні функції включають в себе:
    1. Реєстрація: призначення S-CSCF користувачеві, який виконує реєстрацію SIP.
    2. Потоки сеансів: маршрутизація запиту SIP, отриманого з іншої мережі, в S-CSCF або маршрутизація внутрідоменних запитів SIP між користувачами на різних S-CSCF.

    Використання ресурсів

    Діє як приховуванні топології мережевого шлюзу (THIG): випадок I-CSCF, який приховує конфігурацію, ємність і топологію мережі ззовні. P-CSCF пересилає SIP-повідомлення, отримані від призначеного для користувача устаткування, в функцію управління сеансом викликає виклику (I-CSCF) і / або функцію управління сеансом обслуговуючого виклику (S-CSCF), в залежності від типу повідомлення і процедури. I-CSCF забезпечує точку контакту в мережі оператора, що дозволяє абонентам цього оператора мережі та абонентам, що знаходяться в роумінгу, реєструватися. Після реєстрації S-CSCF підтримує стан сеансу для всіх послуг IMS.

    Рівень також включає в себе інші елементи, в тому числі Домашній сервер абонента (HSS) або серверну функцію профілю користувача (UPSF), яка містить інформацію, пов'язану з підпискою, виконує аутентифікацію та авторизацію користувачів та надає інформацію про фізичну місцезнаходження користувача. Коротше кажучи, база даних Maser.

    BGCF (функція управління прикордонним шлюзом): використовується для вибору мережі, в якій буде встановлено з'єднання з телефонною мережею загального користування. Він або пересилається іншому BGCF, або MGCF, контролюючому доступ для PSTN. MGCF (функція управління медіа-шлюзом): вона керує управлінням викликами медіа-шлюзу, яке повинно відправляти та отримувати дзвінки з або в PSTN або мережу з комутацією каналів. Він використовує повідомлення SIP в / з CSCF / BGCF і використовує повідомлення управління медіа-шлюзом в / з медіа-шлюзу.

MGW (Media Gateway): відповідає за обробку мультимедіа для викликів в PSTN / мережу з комутацією каналів.

MRF (функція медіаресурсу) забезпечує функції, пов'язані з медіа, такі як маніпулювання медіа. Контролер функцій медіаресурсу (MRFC): вузол площині сигналізації, який діє як користувальницький агент SIP для S-CSCF і який управляє MRFP. Медіа-ресурсний процесор функцій (MRFP): вузол медіаплоскості, що відповідає за реалізацію медіа-функцій.

3. Рівень сервера додатків

Контроль кінцевих сервісів, вказані користувачем, здійснюється на рівні сервера додатків.

Сервери, підтримувані на цьому рівні:

- Сервер додатків телефонії (TAS). Сервер додатків телефонії (TAS) є послідовним агентом користувача SIP, який підтримує стан виклику. TAS містить службову логіку, яка забезпечує базові послуги обробки викликів, включаючи аналіз цифр, маршрутизацію, настройку виклику, очікування виклику, переадресацію виклику, конференц-зв'язок і т. Д.
- Мультимедіа IP - функція комутації послуг (IM-SSF): забезпечує взаємодію повідомлення SIP з відповідними налаштованим додатками для розширеної логіки мобільних мереж (CAMEL), ANSI-41, протоколу інтелектуальних мережевих додатків (INAP) або прикладної частини можливостей транзакцій (TCAP) повідомлення.
- Додатковий сервер додатків телефонії: автономні незалежні сервери, які надають додаткові послуги телефонії на початку виклику, в кінці або в середині за допомогою тригерів.
- Сервер додатків без телефонії. Ці сервери додатків взаємодіють з клієнтами кінцевих точок для надання таких послуг, як IM, PTT або служби з підтримкою присутності.
- Відкритий доступ до сервісу - шлюз (OSA-GW). Взаємодія між SIP і API-інтерфейсом Parlay забезпечується у відкритому доступі до сервісів - шлюз (OSAGW), який є частиною рівня сервера додатків архітектури IMS 3GPP.

2.3. Основні елементи IMS і їх функції

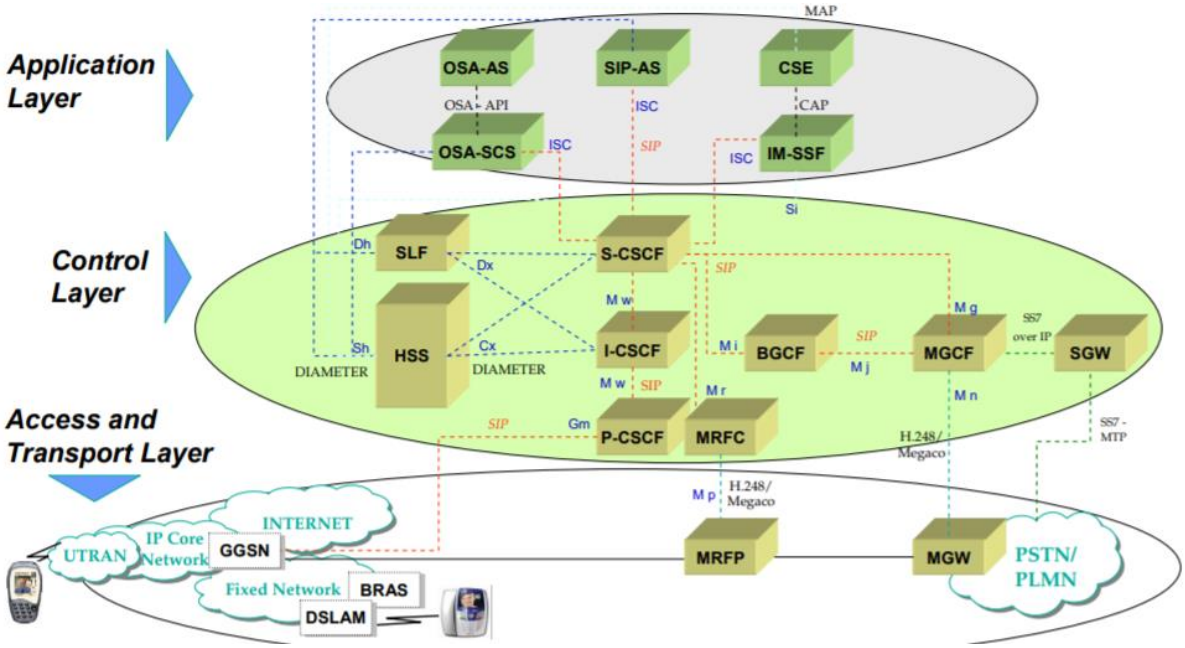

РИС. 2.2. Архітектура IMS визначає елементи і функції на трьох рівнях.

Основний мережевий елемент IMS: CSCF

Call session control function.

Типи SIP-серверів, CSCF, використовуються для обробки пакетів сигналізації SIP в домені IMS:

- P-CSCF
- I-CSCF
- S-CSCF

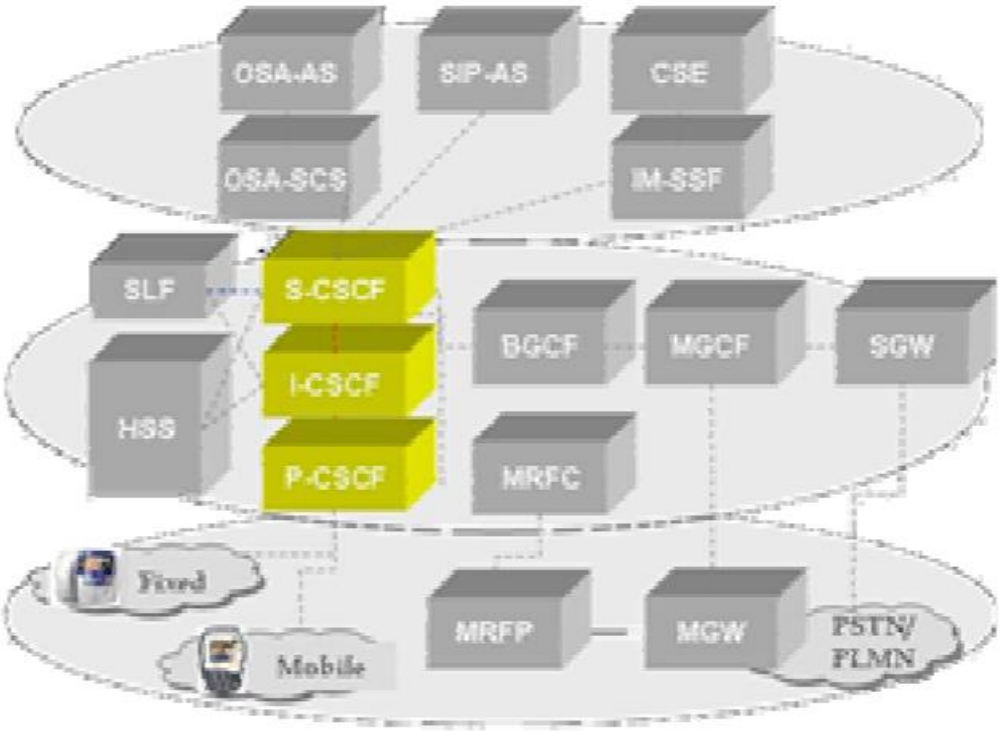

РИС. 2.3. CSCF

Елементи CSCF відповідають за управління сеансом SIP і реалізують логіку для наступних функцій:

- ідентифікація користувача;
- маршрутизація викликів;
- управління формуванням записів відомостей про дзвінки (CDRs) для цілей бухгалтерського обліку;

Кожна мережа, як правило, має кілька CSCF кожного типу, що дозволяє спільно використовувати навантаження і підтримувати підвищену надійність за рахунок використання резервних серверів.

Всі CSCF будуть використовувати протокол ініціалізації сеансу (SIP) в якості протоколу сигналізації. Взаємодія з іншими доменами з використанням різних протоколів здійснюється виділеними елементами.

Основний мережевий елемент IMS: P-CSCF

Proxy Call Session Control Function.

P-CSCF є першою точкою доступу для терміналу до IMS і виконує наступні основні функції:

- перенаправляє заявки на реєстрацію, отримані від UE, в I-CSCF
- перенаправляє повідомлення SIP S-CSCF, який адмініструє користувача, чию адресу визначений під час реєстрації
- переадресує запит та відповіді в УП

P-CSCF призначається терміналу під час реєстрації, призначається або через DHCP, або в контексті PDP і не змінюється протягом реєстрації.

Знаходиться на шляху всіх сигнальних повідомлень, і може перевірити кожне повідомлення.

Перевіряє справжність користувача та встановлює зв'язок безпеки IPsec з терміналом IMS. Це запобігає спуфінг атакам та захищає конфіденційність користувача.

Може стискати і розпаковувати SIP-повідомлення за допомогою SigComp, що зменшує час обходу з повільним радіоканалах.

Може включати PDF (функція прийняття рішень), яка дозволяє використання ресурсів медіаплощини, наприклад якість обслуговування (QoS) на медіаплощині. QoS використовується для керування, управління смугою пропускання і т. д... PDF також може бути окремою функцією.

Основний мережевий елемент IMS: I-CSCF

Interrogating Call Session Control Function.

I-CSCF-це SIP функція, розташована на межі керуючого домену.

- IP-адреса публікується в DNS домені (з використанням записів DNS NAPTR і SRV), так що віддалені сервери можуть знайти його і використовувати в якості точки пересилання (наприклад, реєстрації) SIP-пакетів для цього домену.

- I-CSCF запитує HSS, використовуючи інтерфейс DIAMETER Cx, щоб отримати розташування користувача (інтерфейс Dx використовується від I-CSCF до SLF, щоб знайти необхідний HSS), і потім направляє запит SIP до призначеного S-CSCF.

Основний мережевий елемент IMS: S-CSCF

Serving Call Session Control Function.

S-CSCF є центральним вузлом сигнальної площині.

Це SIP-сервер, завжди розташований у домашній мережі. S-CSCF використовує інтерфейси Cx і Dx до HSS для завантаження і вивантаження профілів користувачів - у нього немає локального сховища користувача. Уся необхідна інформація завантажується з HSS .

- він обробляє реєстрацію SIP, що дозволяє йому пов'язувати розташування користувача (наприклад, IP-адреса терміналу) та SIP-адресу;
- він розташований на шляху всіх сигнальних повідомлень, і може перевірити кожне повідомлення;
- він вирішує, на який сервер додатків буде надіслано повідомлення SIP, щоб надати свої послуги;
- він надає послуги маршрутизації, як правило, використовуючи перерахування пошуків це забезпечує дотримання політики оператора мережі
- у мережі може бути кілька S-CSCFs з причин розподілу навантаження і високої доступності.

Основний мережевий елемент IMS: HSS або UPSF

Домашній абонентський сервер HSS або сервер профілів користувачів функція UPSF

HSS-це база даних всіх абонентських і сервісних даних.

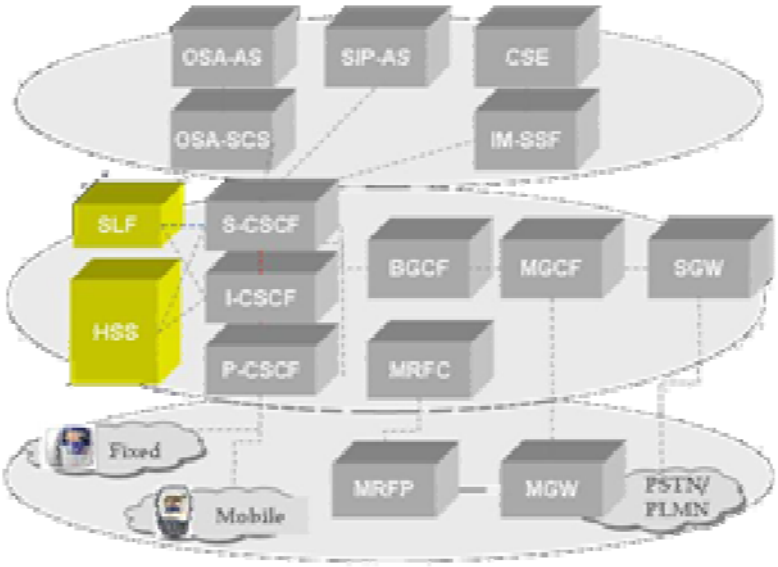

РИС. 2.4 Елементи HSS і SLF.

HSS - це головна база даних користувачів, яка підтримує мережеві об'єкти IMS, які обробляють сеанси викликів:

- Вона містить інформацію, що стосується підписки (профілів користувачів), використовувану рівнем управління.
- Вона надає дані, які використовуються для виконання автентифікації та авторизації користувача
- Вона може надати інформацію про фізичне місцезнаходження користувача

HSS також надає функції традиційного регістра домашнього місцезнаходження (HLR) та Центру аутентифікації (AUC).

Це дозволяє користувачеві отримати доступ до доменів пакетів і каналів мережі спочатку, через аутентифікацію IMSI.

Профіль користувача складається з::

- Посвідчення користувача.
- Виділене ім'я S-CSCF.
- Реєстраційна інформація і профіль роумінгу.
- Параметри автентифікації
- Контроль та службова інформація.

Основний мережевий елемент IMS: SLF

Функція Локатора Підписки (Subscription Locator Function).

SLF необхідний для зіставлення адрес користувачів, коли використовується кілька HSS.

Функція локатора підписки (SLF) використовується в мережі IMS як механізму дозволу, який дозволяє I-CSCF, S-CSCF і AS знайти адресу HSS, який містить дані користувача для конкретного посвідчення користувача, коли в оператора в мережі в наявності декілька HSS.

SLF не виконує ніякої логіки на своїх інтерфейсах, але відповідає на запит з повідомленням перенаправлення, вказуючи адресу HSS, який в змозі виконати отриманий запит.

І HSS, і SLF взаємодіють через протокол DIAMETER.

Основний мережевий елемент IMS: MRF

Функція Медіа-Ресурсу (Media Resource Function)

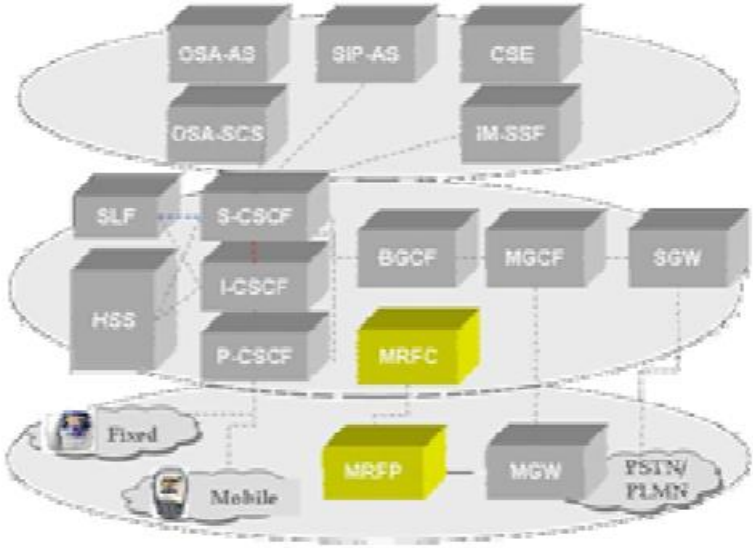

РИС. 2.5. Елемент MRF.

MRF - це функція для курування ініційованих мережевих медіа потоків в домашній мережі.

Вона використовується для :

- Відтворення аудіо / відео повідомлень.
- Мультимедійних конференцій (наприклад, змішування аудіопотоків)
- -Перетворення тексту в мову (TTS) і розпізнавання мови.
- Транскодування мультимедійних даних в реальному часі (тобто перетворення між різними кодеками)

Кожен MRF додатково ділиться на :

- MRFC (Media Resource Function Controller) є вузлом сигнальної площині, який діє як SIP агент користувача до S-CSCF, і який контролює MRFP з інтерфейсом H. 248
- MRFP (Processor Function Processor Function Processor) - це вузол медіа-площини, який реалізує всі функції, пов'язані з медіа.

Основний мережевий елемент IMS: BGCF

Break Out Gateway Control Function.

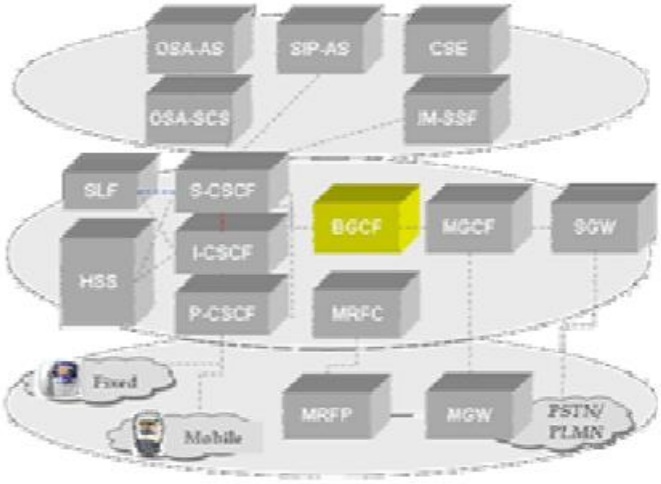

РИС. 2.6. BGCF

BGCF є елементом IMS, який вибирає мережу, в якій повинен відбутися доступ ТМЗК. BGCF використовується для дзвінків з IMS на телефон в комутованій мережі, наприклад, PSTN або PLMN. BGCF пересилає сигналізацію до вибраної мережі PSTN / PLMN.

Якщо доступ відбувається в тій же мережі, що і BGCF, тоді BGCF використовує MGCF (Media Gateway Control Function), яка буде відповідати за взаємодію з PSTN, і передає сигнал MGCF. В іншому випадку він передає сигнал BCGF іншой мережі операторів.

MGCF отримує SIP-сигнал від BGCF і управляє взаємодією з мережею PSTN.

Основний мережевий елемент IMS: шлюзи ТМЗК

Шлюзи Телефонної Мережі Загального Користування.

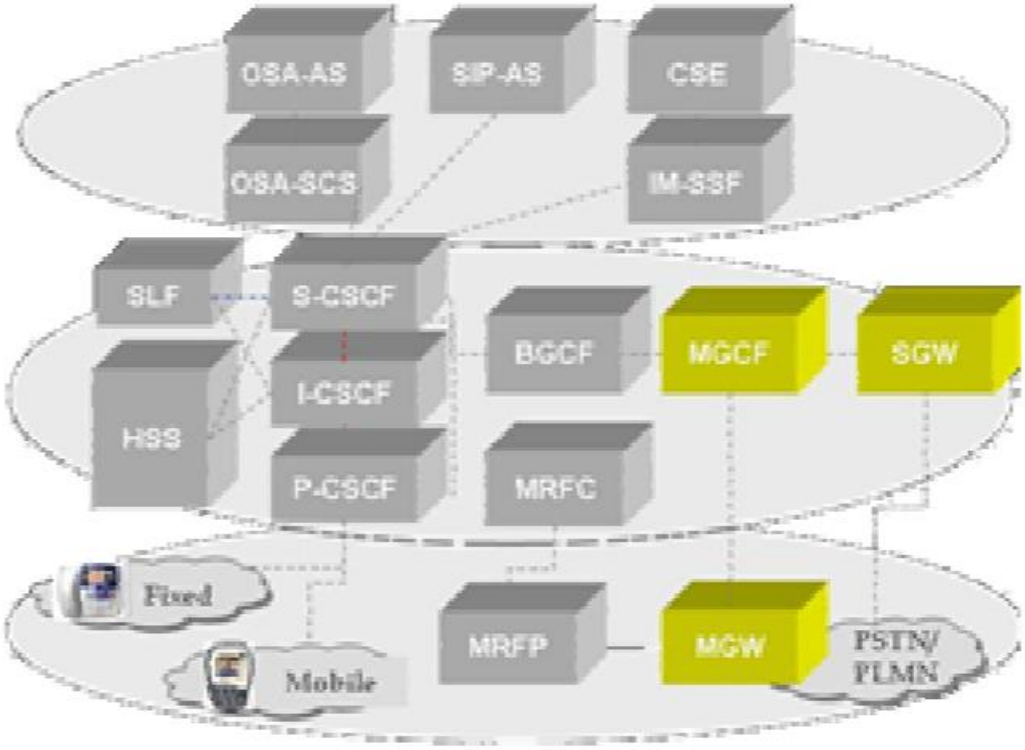

РИС. 2..7. PSTN Geteways.

Взаємодія з мережею з комутацією каналів здійснюється декількома компонентами, для сигналізації, засобів масової інформації та функцій управління:

SGW (Signalling Gateway) - це інтерфейс з сигнальною площиною мережі з комутацією каналів (CS). Він перетворює протоколи нижнього рівня такі як SCTP (який є IP-протоколом) в MTP (який є протоколом SS7), щоб передати ISUP від MGCF до мережі CS.

MGCF (функція контролера медіа-шлюзу)

- Виконує перетворення протоколу управління викликами між SIP і ISUP
- інтерфейси SGW через SCTP
- управління ресурсами MGW з інтерфейсом H. 248.

MGW (Media Gateway)

- Виконує взаємодію площини засобів мережі CS, шляхом перетворювати між RTP і PCM.

– Він також може виконувати транскодування мультимедіа, коли використовувані кодеки не збігаються (наприклад, IMS може використовувати AMR, PSTN може використовувати G. 711).

Основний мережевий елемент IMS: AS

Сервер додатків (Application Servers).

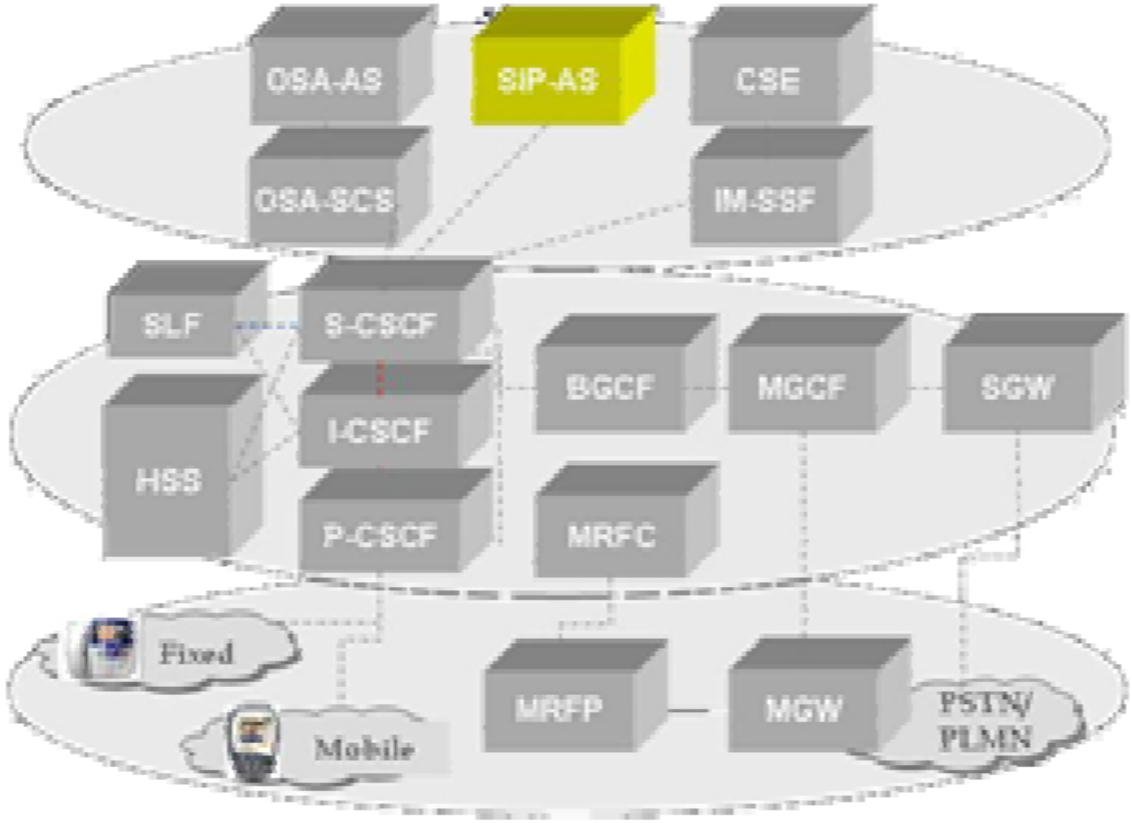

РИС. 2.8. Application Servers.

Сервери додатків розміщують і виконують служби, а також взаємодіють з S-CSCF за допомогою SIP. Це дозволяє стороннім постачальникам легко інтегрувати і розгортати свої додаткові послуги в інфраструктуру IMS.

Прикладами послуг є:

- Послуги, пов'язані з ідентифікатором абонента (CLIP, CLIR, ...).
- Очікування виклику, утримання виклику, виклик забрати.
- Переадресація виклику, передача виклику.
- Послуги блокування викликів, шкідлива ідентифікація абонента.
- Законне перехоплення.
- Анонси, збір цифр.
- Послуги конференц-зв'язку
- Послуги на основі місцезнаходження.
- SMS, MMS.
- Інформація про присутність, обмін миттєвими повідомленнями.

- Функція безперервності мовного виклику (сервер VCC) або фіксована мобільна конвергенція.

Основний мережевий елемент IMS: IM-SSF

IP мультимедіа - функція комутації послуг (IP Multimedia - Service Switching Function)

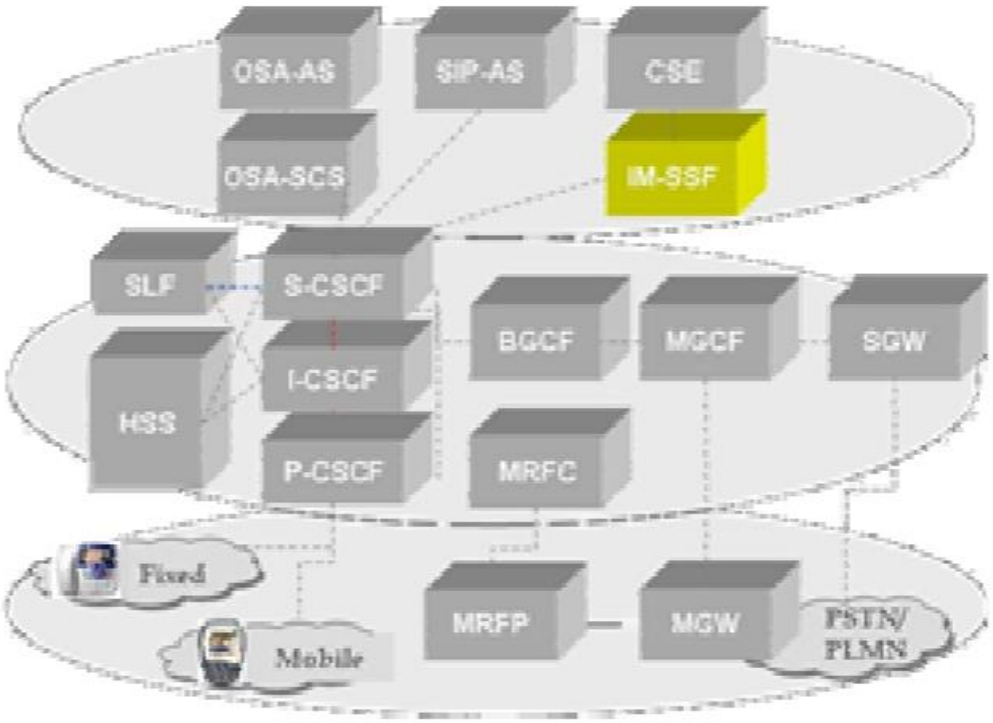

РИС. 2.9. IP мультимедіа - функція комутації послуг.

IM-SSF є вузлом в домені IMS, який забезпечує взаємодію між управлінням сеансом SIP та інтелектуальною мережею традиційних мереж . Він дозволяє направляти запити на обслуговування на застарілі платформи надання послуг, такі як вбудовані SCP.

IM-SSF забезпечує інтелектуальну функціональність шлюзу між мережею IMS на основі SIP і в системах, що використовують такі протоколи, як CAMEL, INAP, AIN і MAP. Ця функціональність має вирішальне значення для розгортання нових, комплексних пропозицій, продовжуючи обслуговувати клієнтів.

IM-SSF також забезпечує доступ до інформації абонента, отриманої з HSS по інтерфейсу Si за допомогою протоколу MAP.

2.4. Стандартизація IMS

Стандартизація архітектури IMS фокусує увагу широкого кола міжнародних організацій, що зумовлено ключовою роллю IMS в еволюції

мереж. Концепція IMS в її нинішньому вигляді в основному є результатом роботи трьох міжнародних організацій зі стандартизації-3GPP, 3GPP2 та ETSI.

Партнерство 3GPP було створене наприкінці 1998 року з ініціативи Інституту ETSI з розробки технічних умов та стандартів для мереж мобільного зв'язку третього покоління (UMTS) на основі розвиваючих мереж GSM.

Партнерство 3GPP2 також було ініційовано в 1998 році ETSI та Міжнародним союзом електрозв'язку (ITU) з розробки мережевих стандартів 3G (мережі CDMA-2000) у рамках проекту IMT-2000, створеного під егідою MCE. Він був утворений майже тими ж організаціями, що і у випадку з 3GPP. Основним внеском організації 3GPP2 у розробку стандартів мобільних мереж 3G стало розширення концепції IMS на мережі CDMA2000 (IP-транспорт, SIP-сигналізація), описане в специфікації під загальною назвою MultiMedia Domain (MMD).

Обидва партнерства розробляють мережеві стандарти 3G, орієнтуючись на широке використання протоколів, орієнтованих на IP, стандартизованих Комітетом IETF, та використання основних ідей архітектури SSP.

Концепція IMS була вперше представлена у випуску 3GPP 5 (березень 2002 р.). він заявив про свою головну мету - підтримку мультимедійних послуг у мобільних мережах на основі протоколу IP - та визначені механізми взаємодії мобільних мереж 3G на основі архітектури IMS з бездротовими мережами 2G.

Мережева архітектура 3G відповідно до концепції IMS має кілька рівнів (площин), розділених на транспорт, управління викликами та рівні додатків. Підсистема IMS повинна бути повністю незалежною від технологій доступу та забезпечувати взаємодію з усіма існуючими мережами - мобільною та стаціонарною, телефонною, комп'ютерною тощо.

У документі 3GPP, випуск 6 (грудень 2003 р.) Було роз'яснено низку положень концепції IMS, додавши питання взаємодії з бездротовими локальними мережами та захисту інформації (за допомогою ключів, абонентських сертифікатів).

Випуски 6 та 7 визначають ідеологію IP-комунікацій за допомогою SIP. Згідно з нею, SIP починається безпосередньо з мобільного терміналу.

Специфікація випуску 7 додає дві основні функції, які є ключовими у фіксованих мережах:

● мережеве вкладення, яке забезпечує механізм аутентифікації абонентів і необхідне у фіксованих мережах, оскільки вони не мають SIM-карт для ідентифікації користувача;

● Ресурс прийому, який резервує мережеві ресурси у фіксованих мережах для забезпечення сеансів зв'язку.

Роботи, спрямовані на розширення концепції IMS наземних ліній, що проводиться Комітетом TISPAN. Інтерес до архітектури IMS з боку ETSI призвів до створення нової робочої групи (2003), яка об'єднала відому групу TIPHON (Узгодження телекомунікацій та Інтернет-протоколів через мережі) та Технічний комітет SPAN (Послуги та протоколи для розширених мереж) , яка відповідає за стандартизацію нерухомих мереж.

Нова група під назвою TISPAN (Телекомунікаційні та Інтернет-конвергентні сервіси та протоколи розширених мереж) відповідає за

стандартизацію сучасних і вдосконалених конвертованих мереж, включаючи VoIP, а також все, що стосується архітектури IMS.

2.5. Актуальність використання IMS в LTE .

Технологія IMS дозволяє використовувати нові послуги зв'язку в мережах фіксованого та мобільного зв'язку і повністю забезпечує їх взаємодію з зовнішніми мережами, дозволяючи скоротити витрати операторів на будівництво інфраструктури.

IMS дає можливість скоротити час установки з'єднання в мережі LTE в 6 разів до 1-2 секунд, передавати голос з високою якістю (HD-voice), вивести на новий рівень якості та доступності контентні послуги, а також дозволить абонентам, чиї смартфони підтримують VoLTE, одночасно говорити по телефону і користуватися високошвидкісним мобільним інтернетом. Голосові виклики, ініційовані в мережі LTE, здійснюються в LTE мережі по IP на базі IMS-платформи (VoLTE).

У разі втрати LTE покриття голосовий виклик перенаправляється в 2G / 3G мережу комутації каналів (CS-voice). Для цього необхідна активація функціоналу Single Radio Voice Call Continuity.

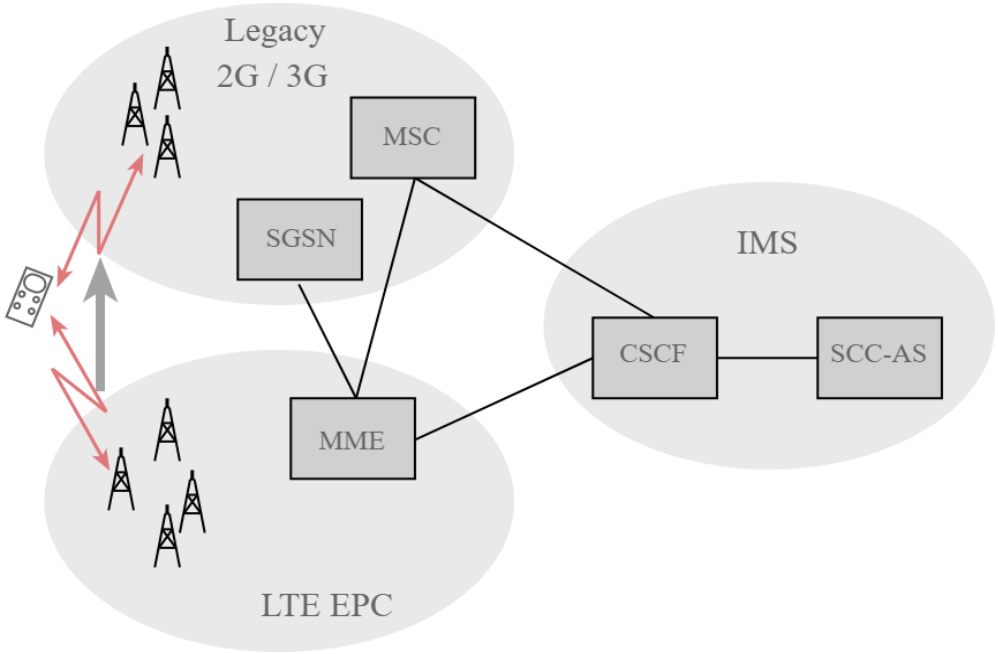

РИС. 2.3. Принцип функціонування Single Radio Voice Call Continuity.

Застосування технології SRVCC дозволяє скоротити час встановлення голосового з'єднання в середньому до 1-ої секунди. Більш того, технологія дозволяє поліпшити якість голосового сервісу на 10-15%, ніж у мережі 2G / 3G.

Окрім голосового зв'язку по мережах передачі даних IMS дає можливість робити дзвінки по мережах Wi Fi (VoWiFi) та фіксованого інтернету (Voice over

Broadband), передавати по мережах LTE відеосигнал (ViLTE), а також реалізовувати технологію RCS - стандарт, що дає можливість операторам запускати власні інтернет-месенджери.

Скорочення часу виходу на ринок нових мультимедійних послуг: інфраструктура IMS забезпечує стандартизовану платформу і повторно використовувані компоненти. Стандартизований інтерфейс і загальні функції, що надаються інфраструктурою IMS, допомагають постачальнику послуг в короткі терміни виводити на ринок нові мультимедійні послуги.

Якість обслуговування (QoS): IMS визначає якість обслуговування в IP-мережі і, таким чином, використовує механізм QoS для поліпшення і гарантії якості передачі.

IMS дозволяє всім службам бути доступними незалежно від місця розташування користувачів: IMS використовує інтернет-технології та протоколи, щоб дозволити користувачам переміщатися по країнах і при цьому мати можливість виконувати всі служби. Отже, всі сервіси доступні користувачеві незалежно від місця розташування.

2.6. Послуги в IMS.

Архітектура IMS-системи передбачає можливість використання її елементів для надання безлічі послуг і роботи безлічі додатків. Це дозволяє скоротити як капітальні витрати на обладнання та комплектуючі, ПЗ, так і витрати, пов'язані з їх обслуговуванням і технічною підтримкою. Впровадження принципово нового сервісу вимагає побудови відповідної інфраструктури для його доставки на відміну від традиційних систем, в яких засоби управління послугами та їх доставки жорстко "пов'язані" з конкретною послугою (наприклад, АТС - телефонія, сервер MCU - відео-конференц-зв'язок і т. п.).

Реалізувавши принципи IMS, оператор може серйозно заощадити і при нарощуванні потужностей своєї мережі. При використанні традиційної - "монолітної" - системи оператор змушений модернізувати її повністю, навіть коли потрібно підвищити ємність (або інші характеристики) тільки одного логічно виділеного функціонального блоку. В "листкової" мережі IMS кожен шар можна нарощувати окремо: транспортний - коли підвищується обсяг трафіку; управління сервісами (сеансами зв'язку) - коли зростає число абонентів і / або сеансів зв'язку; нарешті, прикладної - коли зростає популярність конкретного сервісу або необхідно впровадити новий. Зрозуміло, що при цьому у оператора є широкі можливості по оптимізації своїх інвестицій в нові апаратні і програмні засоби.

Реалізація нових послуг ще одна перевага архітектури IMS. Незалежність IMS від специфіки мережевого транспорту і каналів доступу робить її відмінною основою для конвергенції служб фіксованого та мобільного зв'язку (Fixed Mobile Convergence - FMC). Але тут важливо зауважити, що IMS аж ніяк не єдино можливий технологічний фундамент FMC. Більш того, на початковому етапі конвергенції економічно вигідними, швидше за все, виявляється інші рішення.

Концепція IP Multimedia Subsystem (IMS) має великий вплив на сферу послуг зв'язку додаткової споживчої цінності (Value Added Services - VAS), або

додаткових послуг. Нова технологія обіцяє швидкі і радикальні зміни в способах спілкування людей, їх роботи, споживання ними інформації та розваг.

Рушійною силою цього процесу є не якась специфічна супер послугу, а сукупність послуг. Сьогодні вже зрозуміло, що одна скільки завгодно новаторська послуга зв'язку не здатна спонукати операторів на розвиток інфраструктури IMS, так само як один супер-додаток не може задовольнити всі потреби користувачів. А ось прагнення надавати безліч найрізноманітніших послуг з будь-яких мереж і для будь-яких терміналів штовхає операторів до швидкого ухвалення IMS.

Концепція IMS змінює звичну практику відповіді на виклики. Абонент може відповісти на дзвінок з будь-якого апарату, який опинився в дану хвилину у нього під рукою: зі звичайного, мобільного або IP-телефону, з програмного клієнта або пристрої типу Skype і навіть зі спеціально обладнаного телевізора, підключеного до широкосмугової мережі. При цьому він, в залежності від необхідності, може вибирати будь-який вид комунікацій: обмін текстовими повідомленнями, голосовий або відеозв'язок (наприклад, Push-to-Show) - і, не перериваючи сеансу зв'язку, перемикатися між цими режимами.

Новий сценарій управління викликами виглядає наступним чином: абонент А дзвонить абоненту В. Комутатор ТМЗК надсилає повідомлення сервера інтелектуального управління викликами. Той зв'язується з абонентським пристроєм, що належить абоненту А, на якому з'являється сигнал про виклик і меню доступних способів його обробки. Абонент А може відповісти на дзвінок, прийняти дзвінок на іншому абонентському пристрої, переправити його іншому абоненту, відповісти автоматичним повідомленням, запросити дані про абонента або просто не відповідати на дзвінок.

Мережі IMS включають в себе нові потужні компоненти підтримки послуг: сервери визначення присутності абонента і його місцезнаходження, формування спільнот і інтерактивних Web-технологій (rich media). Ці компоненти надають новий рівень персоналізації послуг і самі нові послуги (розваги, інформація, навчання, онлайнова торгівля і т. Д.), Що значно розширюють можливості абонентів в використанні телекомунікацій. Наприклад, інформація про присутність абонентів в єдиному комунікаційному просторі особливо актуальна в позаурочний час. Так, вночі абонент може перевірити, хто з колег або друзів доступний, чи можна з ким-небудь з них поговорити або ж спілкування буде обмежено тільки можливістю послати їм повідомлення.

Послуги на основі контролю географічного місцезнаходження найбільше затребувані в поїздках, коли абонент отримує можливість ділитися з сім'єю та друзями враженнями про події, що відбуваються в онлайновому щоденнику або блозі, що підтримується засобами створення спільнот і потокової передачі мультимедійної інформації.

Концепція IMS передбачає підключення до будь-яких мереж (стільникового зв'язку, фіксованим, DSL, Wi-Fi, кабельним і т. Д.) І прозоре надання послуг з будь-яких каналах і на будь-які термінали. В результаті користувачі отримують розширений доступ до послуг у будь-яких умовах і відповідно до своїх вимог.

IMS має на увазі горизонтальну архітектуру додатків послуг, що дозволяє поєднане використання мережевих ресурсів, що дає можливість більш ефективно задіяти ресурси і управляти ними, а отже, і знижувати капітальні витрати на створення мереж. У мережах IMS значно зменшаться операційні витрати. Нова концепція дозволить операторам підтримувати безліч послуг, а завдяки універсальним стандартам виросте і швидкість їх впровадження на ринок.

Основним протоколом в IMS є SIP протокол. Заснована на протоколі SIP, архітектура IMS пропонує гнучкі і потужні засоби встановлення та модифікації сеансів мультимедійної зв'язку.

Перелік деяких функцій використовуваних абонентом в IMS:

- PoC - натисніть, щоб говорити по стільниковому зв'язку
- Багаторазові і одночасні дзвінки / знайди мене, йди за мною: дзвінок направляється в заздалегідь визначений список адресатів (послідовно або паралельно)
- Multimedia Push: ця послуга дозволяє користувачам завантажувати мультимедійний контент (наприклад, вітальну листівку)
- Push RingTone: викликає сторона вибирає, який сигнал виклику буде дзвонити на номер / адресу одержувача.
- Обмін відео в реальному часі: одноранговая, потоковая мультимедійна послуга в реальному часі
- Інтерактивні ігри
- Загальні папки: Обмін контентом дозволяє користувачам обмінюватися файлами між терміналами.
- Голосові повідомлення: форма обміну миттєвими повідомленнями, в якій вміст повідомлення являє собою аудіофайл.
- Сервіси миттєвих повідомлень: комунікаційний сервіс, що дозволяє кінцевим користувачам миттєво відправляти і отримувати повідомлення.
- Відеоконференцзв'язок: мультимедійна IP-підсистема (IMS). Служба відеоконференцзв'язку розширює можливості двухточечного відеодзвінка многоточечний сервіс.
- IMS з голосовою і відео телефонії
- сервер присутності IP Centrex
- Потокове медіа і завантажити батьківський контроль
- Екран вхідних викликів і програмований контроль
- Заборона / контроль вихідних дзвінків VoIP
- Конвергентна система миттєвих повідомлень (мікшування SIP, USSD, SMS, перетворення тексту в мову)
- Контролер розширеної політики (перевіряє і контролює послідовності і формат повідомлень SIP)

2.7. Висновки до розділу

У даному розділі розглянуто структуру та роль мультисервісної IP підсистеми (IMS) як у сучасних телекомунікаційних системах, так і її перспективу і доцільність використання у майбутньому.

Отже, можна зробити висновок, IMS: дає можливість підключити набагато більше абонентів, ніж на софтсвіч, тому що навантаження розподілене, тобто за обробку дзвінків відповідають сервера. Введена функція контролера за проксі-серверами. S-CSCF виконує функцію контролера за проксі-серверами. Софтсвіч за трафік не відповідає. З'явилася масштабованість. Ми можемо забезпечити (підключити) більше абонентів. З'явилася можливість забезпечувати більшу кількість доступу до сервісів, послуг, контенту. IMS – більш гнучка система, тобто кожний вузол цієї архітектури – незалежний елемент.

Також, в рамках даного розділу наводиться інформація про актуальність і послуги, що надаються в сучасних мобільних мереж 4G LTE та їх безпосередній зв'язок з підсистемою IMS.

Розділ 3. Процес обслуговування абонентів в мережах IMS.

3.1. Реєстрація користувача в мережі IMS

Мультимедійна підсистема IP забезпечує площину управління з використанням серверів функції управління сеансами виклику (CSCF) за допомогою протоколу ініціалізації сеансу (SIP). Дані користувача управляються домашнім сервером абонента (HSS) і центром аутентифікації (AuC). IMS визначає наступні типи серверів CSCF. Проксі-CSCF (P-CSCF), перший перехід у відвідуваній мережі, який перенаправляє повідомлення SIP від абонента до домашньої мережі.Він також встановлює зв'язок безпеки IPSEC з терміналом. Ключі конфіденційності і цілісності, *Ck i Ik* відповідно, виходять в результаті аутентифікації, виконаної за допомогою HSS і переданої в P-CSCF за допомогою сигналізації. I-CSCF, розташований у домашній мережі, яка знаходить сервер, здатний керувати абонентськими повідомлення SIP. Нарешті, S-CSCF , обслуговуючий CSCF, аутентифікує абонентів, які отримують доступ аутентифікації від HSS.

Аутентифікація IMS заснована на HTTP Digest Authentication, використовуючи алгоритм AKAv1-MD5, який вимагає обміну чотирма повідомленнями (2 рази в обидва кінці-RTT) між абонентом, відвідуваної мережі і домашньої мережі абонента.

Аутентифікація IMS спирається на UICC (універсальну інтегральну схему), смарт-карту, розташовану у абонента, яка містить ISIM (модуль віртуального абонента). Протокол реєстрації IMS працює наступним чином (рис. 3.1)

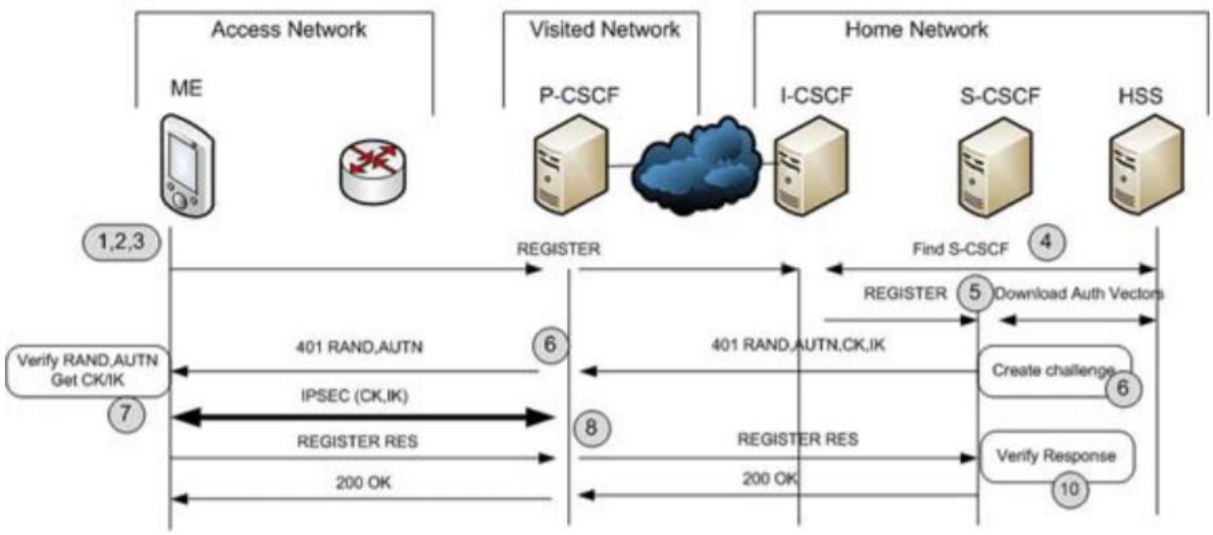

РИС. 3.1. Обмін повідомлень для успішної реєстрації в IMS.

1. Мобільний елемент (ME) реєструється у мережі доступу і виявив P-CSCF.
2. На кроці 2 ME використовує UICC для отримання інформації про абонента реєстраційний URI (щоб знайти домашню мережу), публічну / приватну особу та контакту адресу для створення повідомлення SIP REGISTER. Більше того, МП включає захисні заголовок клієнта із зазначенням, які алгоритми IPSEC підтримуються.
3. ME відправляє вищезгадане повідомлення REGISTER до P-CSCF, яке вставляє мережу P-Visited-Network дентифікатор у повідомленні РЕЄСТР. P-CSCF зчитує та видаляє захист-клієнтський заголовок і перенаправляє повідомлення REGISTER на виявлений I-CSCF (в домашню мережу).
4. I-CSCF знаходить відповідний S-CSCF для обробки повідомлень ME надсилаючи запит на аутентифікацію користувача діаметром (UAR) до HSS.
5. Повідомлення REGISTER доходить до S-CSCF. S-CSCF завантажує автентифікатори для абонента від HSS. Ці вектори містять параметри для аутентифікації та виведення ключів з використанням AKA як: випадковий виклик (RAND), маркер аутентифікації (AUTN), очікувана відповідь ME (XRES), Tegrity (*Ik*) та ключ конфіденційності (*Ck*). AUTN виводиться за допомогою HSS. На 5 кроці відбувається створенням S-CSCF 401 Несанкціоноване повідомлення, WWW- Аутентифікаційний заголовок, що містить AUTN та RAND. S-CSCF включає також *Ck* і *Ik* у повідомленні, яке слід прочитати P-CSCF. S-CSCF надсилає це повідомлення, яке повернулося до ME.

6. На кроці 6 повідомлення 401 несанкціонованого доступу доходить до P-CSCF в гостовій мережі. P-CSCF витягує та видаляє *Ck* та *Ik* із повідомлення (ME отримують *Ck* і *Ik* від AUTN і RAND за допомогою UICC) і додають Security-Server заголовок вибору одного алгоритму IPSEC з запропонованого клієнтом на кроці 2.
7. ME отримує повідомлення 401 і використовує UICC, для виклику сформулюйте відповідь на виклик (RES), *Ck* і *Ik* від AUTN та RAND. Тоді ME встановлює асоціацію безпеки з P-CSCF за допомогою *Ck* / *Ik* і створює нове REGISTER повідомлення, що містить RES та заголовок Security-Verify. Тоді він пересилає повідомлення P-CSCF щодо абсолютно нової асоціації безпеки IPSEC.
8. P-CSCF, після отримання повідомлення по захищеному каналу, підтверджує ME. Потім він перенаправляє повідомлення до I-CSCF.
9. Повідомлення передається до S-CSCF.
10. S-CSCF отримує REG-Повідомлення ISTER і перевіряє, чи відповідає RES XRES для автентифікації абонента. Якщо користувач успішно проходить автентифікацію, S-CSCF створює повідомлення 200 OK і надсилає його до ME, закінчуючи процес реєстрації IMS.

Коли обладнання користувача зареєстровано, воно може ініціювати і приймати сесії. При повторній реєстрації аутентифікація користувача не потрібно (рис. 3.2.).

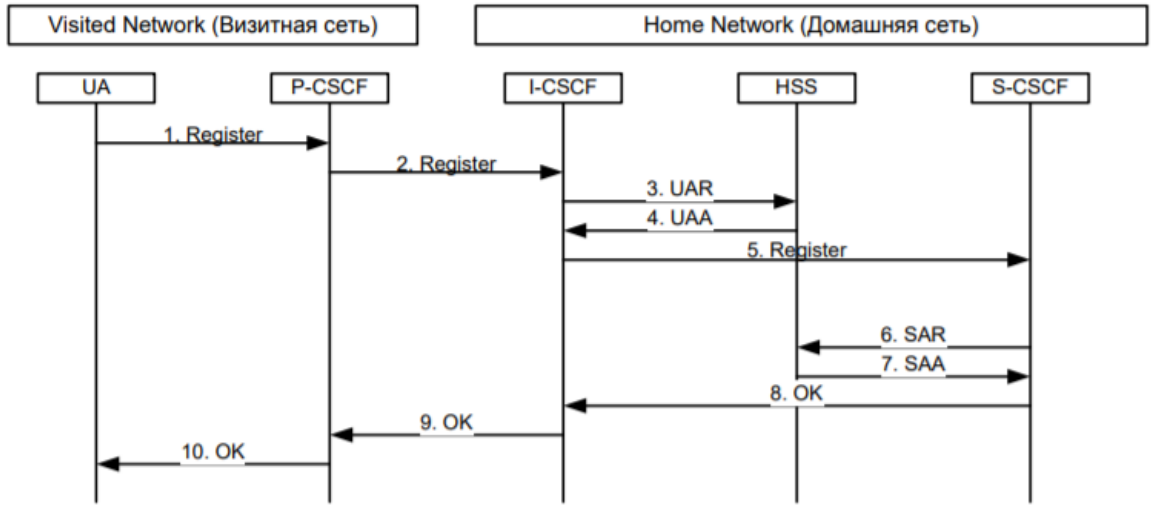

РИС. 3.2. Процес реєстрації користувача в мережі IMS.

Інформація, що зберігається в елементах мережі IMS до, під час і після процесу реєстрації ME представлена в табл. 1

Таблиця 1

Елемент мережі, ME	До реєстрації	Під час реєстрації	Після реєстрації
Термінал користувача (UE) –	Обліковий запис з параметрами	Те ж, що до реєстрації	Обліковий запис з параметрами

у гостьовій мережі	доступу користувача, сформованими після його успішної аутентифікації. Адреса домашнього домену. Ім'я/адреса P-CSCF		доступу користувача, сформованими після його успішної аутентифікації. Адреса домашнього домену. Ім'я/адреса P-CSCF
P-CSCF – в домашній або гостьовій мережі	Функція маршрутизації	Початкова точка входу в домашню мережу. Адреса UE. PrUI, PuUI	Фінальна точка входу в домашню мережу. Адреса UE. PrUI, PuUI
I-CSCF – в домашній мережі	Адреса HSS або SLF	Адреса/ім'я S-CSCF. Ідентифікатор мережі P-CSCF. Контактна інформація про домашній мережі	Ніякої інформації про стан
HSS	Профіль послуг користувача	Ідентифікатор мережі P-CSCF	Адреса/ім'я S-CSCF
S-CSCF – в домашній мережі	Ніякої інформації про стан	Адреса/ім'я P-CSCF. Ідентифікатор мережі P-CSCF. PrUI, PuUI. IP-адреса UE. Ідентифікатор GRUU для UE	Може зберігатися інформація про стан сесії. Те ж, що під час реєстрації

Скасування реєстрації користувача в мережі IMS

Процедура скасування реєстрації аналогічна процедурі реєстрації (рис. 3.3.), тільки повідомлення протоколу SIP Register містить заголовок Expires зі

значенням часу реєстрації, рівним нулю, або заголовок Contact з параметром expires рівним нулю.

Реєстрація множинних ідентифікаторів користувача

Протокол SIP дозволяє реєструвати за одну процедуру реєстрації один ідентифікатор PuUI користувача. Таким чином, якщо користувач має кілька ідентифікаторів PuUI, він повинен реєструвати кожен з них індивідуально. Для реєстрації декількох PuUI 3GPP розроблений механізм множинної реєстрації.

Множинна реєстрація дозволяє зареєструвати групу ідентифікаторів PuUI за допомогою одного запиту реєстрації. PuUI ідентифікатори об'єднуються в групи і, коли один з ідентифікаторів групи зареєстрований, все PuUI ідентифікатори, асоційовані з ним, реєструються в цей же момент. Коли для одного з ідентифікаторів скасовується реєстрація, вона скасовується і для всіх ідентифікаторів групи.

3.2. Встановлення сеансу зв’язку в IMS

Сценарій (рис. 3.3.) являє процедуру встановлення мультимедійної сесії між зареєстрованим користувачами IMS, що знаходяться в домашніх мережах.

Користувач User A ініціює виклик до користувача User B. Термінальний обладнання користувача User A відправляє повідомлення INVITE протоколу SIP для запиту встановлення мультимедійної сесії з користувачем User B, що містить опис сесії в форматі SDP для передачі даних від User B до User A (тип переданих даних - відео, аудіо), транспортний протокол (TCP, UDP), формат даних (H.261, MPEG), IP адрес пристрою, адрес порту RTP, використовувані кодеки).

P-CSCFA приймає запит INVITE, замінює в запиті INVITE заголовок P-Preferred-Identity на заголовок P-Asserted-Identity, що містить зареєстрований ідентифікатор PuUI викликає користувача, додає в заголовок Route свою адресу і відправляє запит до функціонального об'єкту S-CSCFA.

До обладнання викликається користувач, P-CSCFA відправляє відповідь з кодом 100 (Trying). Ця відповідь інформує термінал в тому, що запит INVITE був отриманий, і проксі-сервер виконує маршрутизацію запиту до місця призначення.

S-CSCFA на підставі ідентифікатора користувача User B, що міститься в запиті INVITE, визначає вхідну точку в домашню мережу викликається користувача I-CSCFB. Після чого відправляє запит INVITE до I-CSCFB, а до P-CSCFA відповідь 100 (Trying). I-CSCFB обробляє запит
і звертається до бази користувачів HSS для отримання адреса функції SCSCF, яка обслуговує користувача User B (взаємодія з HSS на Мал. 1.8 не представлено).

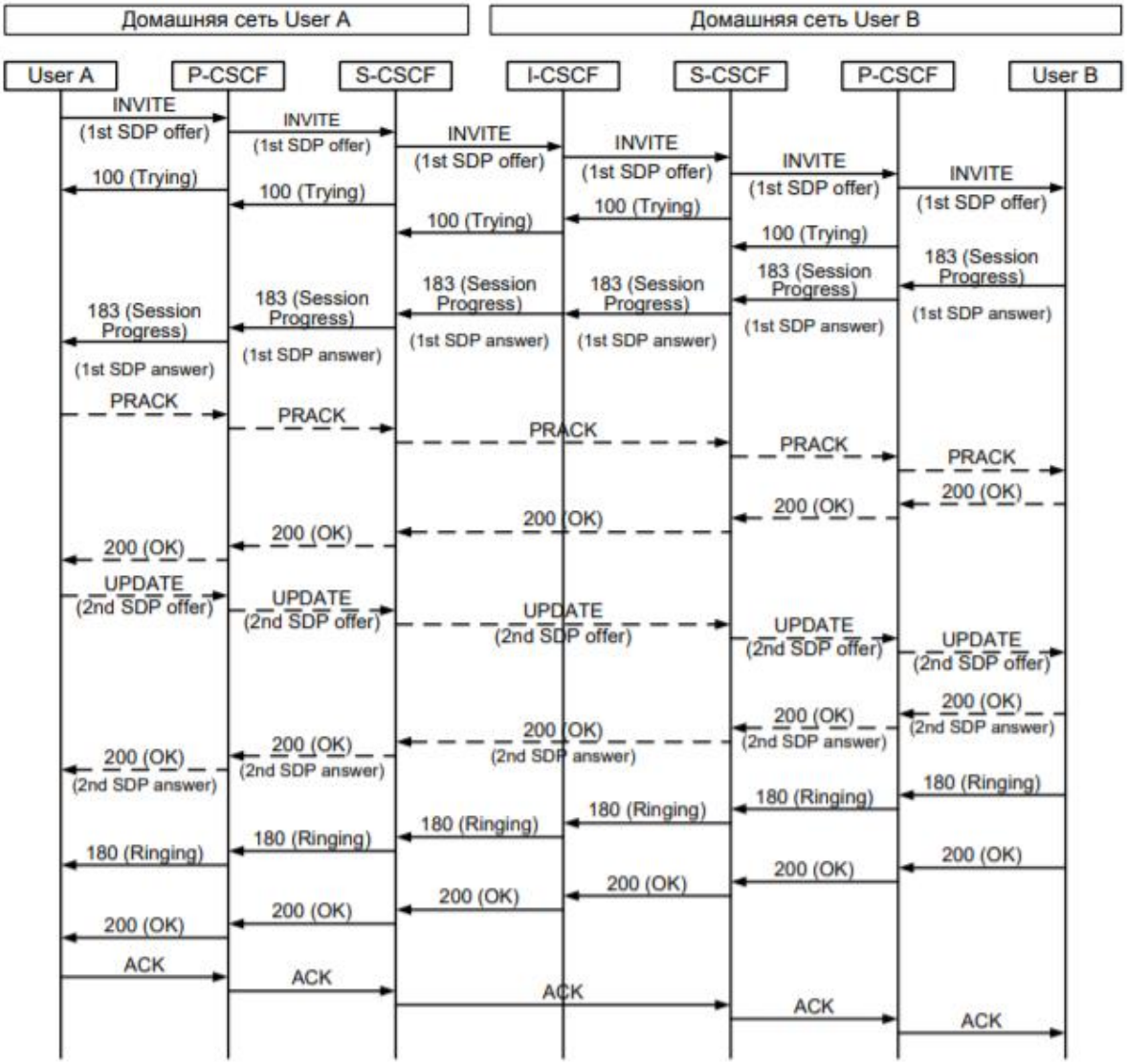

Рис. 3.3. Встановлення мультимедійного сеансу.

Після отримання адреса I-CSCFB передає запит INVITE до функції S-CSCFB, яка формує відповідь 100 (Trying) до I-CSCFB. S-CSCFB передає запит вже до функції P-CSCFB, яка транслює його до терміналу User B. Термінал викликається користувача обробляє запит INVITE і відправляє відповідь 183 Session Progress, що містить SDPопісаніе сесії для передачі мультимедійних даних від User A до User B.

Термінальне обладнання User A, отримавши відповідь 183 Session Progress, аналізує запропоноване SDP-опис сесії і відправляє запит PRACK для інформування викликається користувача User B в обраних параметрах сесії (наприклад, кодеках). Користувач User B підтверджує прийняття запиту PRACK відповіддю 200 OK. потім користувач User A відправляє запит UPDATE для узгодження параметрів якості обслуговування QoS з користувачем User B і отримує підтвердження - відповідь 200 OK. При оповіщені користувача про вхідні виклику термінал користувача User У інформує про це термінал користувача User A за допомогою відповіді з кодом 180 (Ringing), який маршрутизується назад через функціональні об'єкти мережі IMS.

У наведеному прикладі User B вирішує відповісти на виклик. Коли він піднімає трубку, його термінал відправляє відповідь з кодом 200 OK, що

вказують, що виклик прийнятий. При отриманні відповіді з кодом 200 термінал користувача User A припиняє подачу сигналу КПВ і доповідає про те, що викликаймий користувач прийняв виклик.

У підсумки, термінал User A відправляє повідомлення підтвердження ACK, для того щоб підтвердити прийняття остаточної відповіді 200 OK. це підтвердження завершує 3-етапну транзакцію INVITE / 200 / ACK, використовувану для встановлення SIP-сесії. Медіа сесія між User A і User B тепер вважається встановленої.

3.3. Висновки до розділу

Реєстрація є необхідною процедурою при роботі в мережі IMS. Не зареєстровані користувачі не можуть отримати доступ до сервісів мережі. В даному розділі розглянуті такі процедури, як реєстрація користувача
в мережі IMS за умови, що користувач перебуває в гостьовій мережі, і встановлення мультимедійної сесії між зареєстрованим користувачами IMS, що знаходяться в домашніх мережах. Можливі два варіанти процедури реєстрації: з аутентифікацією і без аутентифікації. У разі якщо користувач вперше реєструється в мережі IMS, йому необхідно пройти аутентифікацію. При повторній реєстрації аутентифікація користувача не потрібно. Скасування реєстрації аналогічна процедурі реєстрації, тільки повідомлення протоколу SIP Register містить заголовок Expires зі значенням часу реєстрації, рівним нулю, або заголовок Contact з параметром expires рівним нулю. IMS дає можливість для реєстрації декількох PuUI. Командою 3GPP розроблений механізм множинної реєстрації.

Розділ 4. Передача голосу через Інтернет - протоколу (VoIP). Аналіз продуктивності, QoS заходи для мінімізації втрат пакетів і ідентифікації збоїв з'єднання під час передачі.

VoIP є технологією, яка забезпечує передачу голосу в мережах з пакетною комутацією протоколу IP. Передача голосу по IP мережі являє собою загальний термін, який відноситься до будь-яких засобів перетворення голосових викликів в пакетно голосових даних, які передаються по IP-мережі публічним або приватним
порядком. У VoIP, відстань між передавачем і приймачем не грунтується на географічній відстані. Час передачі залежить від пропускної здатності і прийнятих динамічних алгоритмів маршрутизації.

Однією з проблем використання VoIP є латентність (затримка або довгий час очікування). Коли пакети посилаються різними маршрутами, всі пакети не можуть прибути в один і той же час. Це призводить до затримки. Для того, щоб передати / завантажити повідомлення, всі пакети повинні бути отримані. Навіть якщо один пакет відсутній, повне повідомлення не може бути сформовано. Щоб

подолати цю проблему і зробити передачу настільки ж ефективною, як ТМЗК, ми приймаємо алгоритми динамічної маршрутизації від джерела.

Наступною проблемою є зменшення потенційної можливості з деградацією QoS. Деякі з пакетів можуть бути втрачені через тайм-ауту або відсутності буферного простору. Це призводить до отримання помилкових даних, а також вимагає повторної передачі одного і того ж повідомлення знову і знову. У цьому розділі представляю загальні алгоритми для зменшення часу очікування та динамічні алгоритми маршрутизації для мінімізації втрати пакетів.

Сьогодні передача голосу по мережі з комутацією пакетів (ATM, FrameRelay і IP) є одним з найбільш зростаючих аспектів мережі мультисервісного доступу. Системи VoIP приймають самі різноманітні форми, включаючи традиційні телефонні апарати, конференц-підрозділи і мобільні пристрої. На додаток до обладнання кінцевого користувача, VoIP системи включають в себе ряд інших компонентів, включаючи процесори обробки викликів, шлюзи, маршрутизатори, міжмережеві екрани і протоколи.

Більшість з цих компонентів мають аналоги, що використовуються в мережах передачі даних, але особливістю VoIP являється те, що звичайне мережеве програмне забезпечення і апаратні засоби повинні бути доповнені спеціальними компонентами IP-телефонії.

Перетворення мережевих адрес (NAT) є потужним інструментом, який може бути використаний, щоб приховати внутрішні мережеві адреси і включити кілька кінцевих точок в межах локальної мережі, щоб використовувати один і той же (Зовнішній) IP-адрес. З одного боку, спроба зробити виклик в мережу стає дуже складною, коли застосовується NAT. Ситуація дещо нагадує офісну будівлю, де пошта адресується з іменами співробітників і адресою будівлі, але внутрішня адресація обробляється поштовим відділенням компанії. Є також кілька питань, пов'язаних з передачею голосових даних через NAT, включаючи несумісність з IPsec.

Іншою проблемою IP-мережі є зниження темпу роботи, яке може збільшити затримки, джиттер і втрати пакетів. Зниження темпу роботи може бути викликано багатьма причинами, в тому числі питаннями конфігурації, атаками DoS (відмова в обслуговуванні) або високим коефіцієнтом використання пропускної здатності іншими системами в мережі. Від DoS атаки складно захищатися, але ризик атаки може бути зменшений шляхом фільтрації трафіку, дозволом того трафіку, який може взаємодіяти з мережею. Це може виявитися важкою проблемою, через використання випадкових портів по VoIP.

Основним завданням даного розділу є огляд двох моделей VoIP (H.323 і SIP), і алгоритм TORA (Temporally-Ordered Routing Algorithm) для пакетної передачі даних, щоб мінімізувати затримку.

VoIP (Рис. 4.1.) перетворює кожен зразок в цифрову форму, передає оцифрований потік через Інтернет в пакетах, і перетворює потік назад.

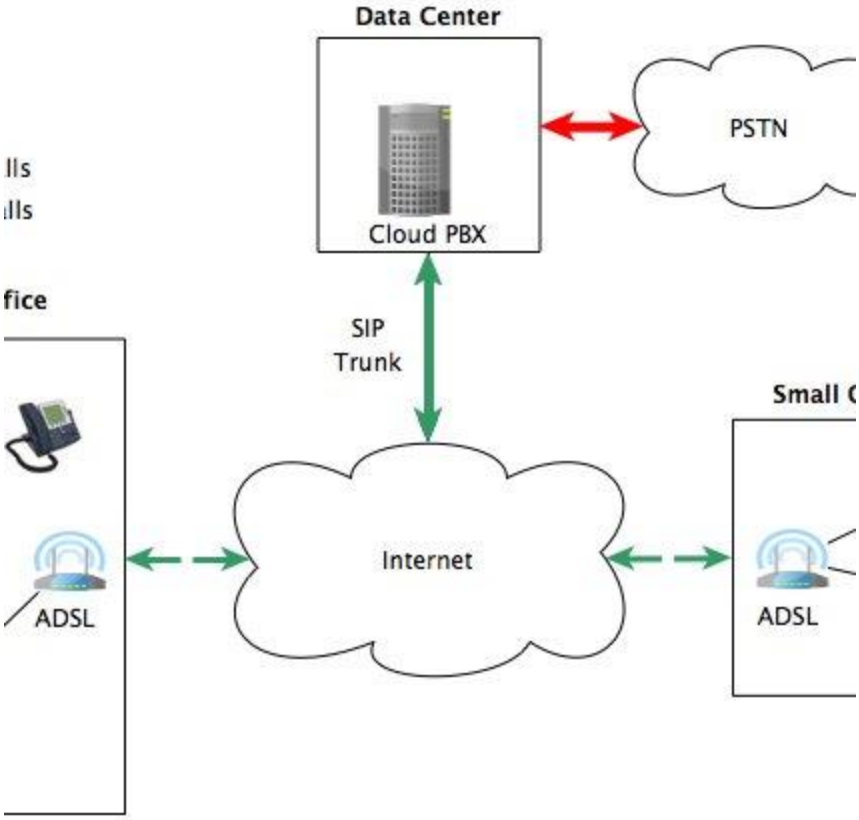

РИС. 4.1. Умовна архітектура VoIP

VoIP H.323 Модель: H.323 є рекомендацією Сектора стандартизації електрозв'язку MCE (ITUT), який визначає протоколи для надання аудіовізуальних сеансів зв'язку з будь-якої мережі з комутацією пакетів. Стандарт H.323 виконує важливі функції управління і сигналізації, обробку звукових і відеосигналів, передачу мультимедійної інформації та забезпечення інформаційної безпеки, управління пропускною спроможністю в конференціях точка-точка і многоточка (рис. 4.2.). Він широко застосовується в устаткуванні аудіо та відеоконференцзв'язку.

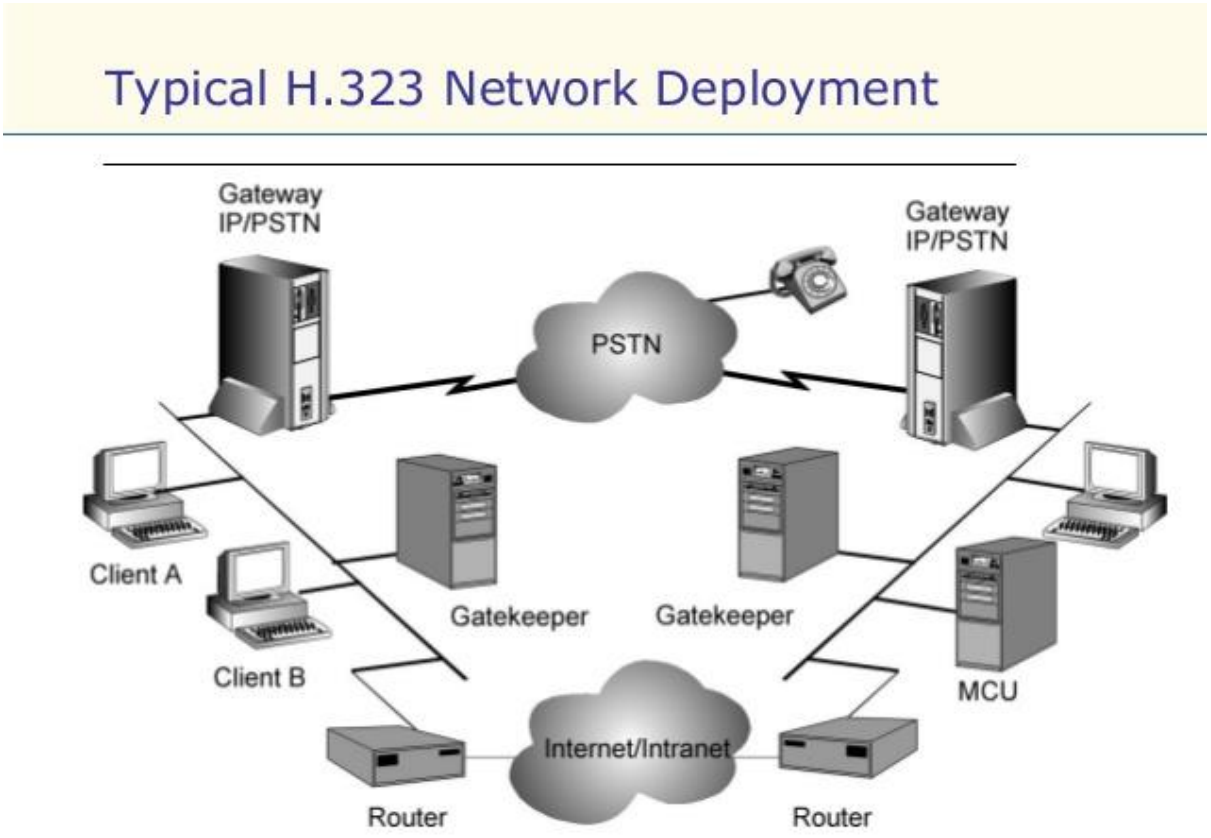

РИС. 4.2. Модель мережі H.323.

SIP Модель: SIP визначає три основні елементи, які складають систему сигналізації (рис. 4.3.):

1. Агент користувача: IP-телефон або додатки
2. Адреса сервера: зберігає інформацію про місцезнаходження або IP-адреса користувача
3. Підтримка серверів: SIP використовує три типи серверів. Типи серверів:

- Проксі-сервер: перенаправляє запити від агентів користувачів.
- Сервер переадресації: визначає поточний адреса викликається користувача.
- Сервер реєстрації: визначає місце розташування користувача в поточний момент часу
- SIP охоплює всі аспекти сигналізації, наприклад, місцезнаходження абонента, дзвінок телефону, відповідь буде і завершення виклику.

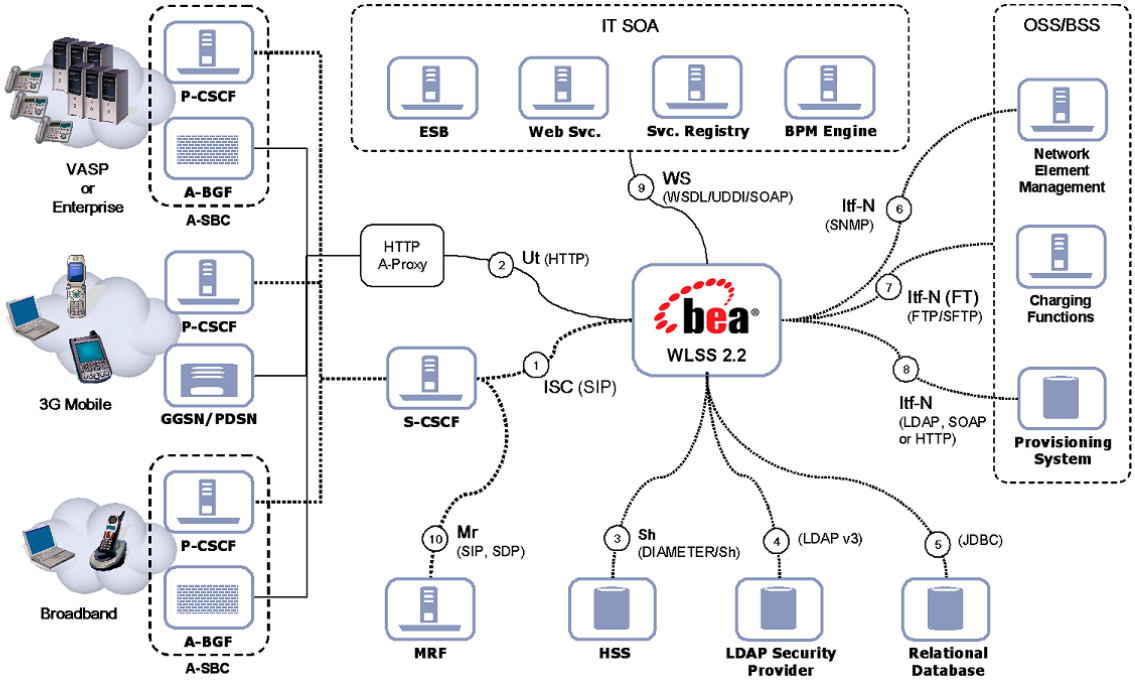

РИС. 4.3. Модель SIP.

Аналіз проблеми

Звичайно, VoIP стикається з багатьма проблемами. Першою і найбільшою з них є затримка. Допустима затримка в телефонії максимально 200 мілісекунд. При більш високих значеннях можуть виникнути труднощі при проведенні розмови. На жаль, доступна смуга пропускання в VoIP НЕ резервується, тому немає гарантованої якості обслуговування (QoS), як в телефонній мережі загального користування. Через замалої доступної смуги пропускання, голосові пакети змушені чекати своєї черги, що буде створювати затримку.

Ще одна проблема виникає, якщо наступні пакети відчувають затримку різної довжини. Приймач повинен зібрати всі пакети, для того, щоб відновити повний потік трафіку і відтворити його користувачеві. Саме тому різниця затримок між пакетами змушує приймач чекати затриманих пакетів, навіть якщо більша частина пакетів вже доступна. Таким чином, навіть якщо середня затримка пакетів по мережі буде відносно невеликою, загальна затримка буде набагато більше. Вона значно збільшиться за рахунок одиночних запізнілих пакетів. Така зміна латентності по мережі називається джиттером. Джіттер може як збільшити загальну затримку, так і створити перерву або періоди мовчання. Це станеться, якщо деякі пакети будуть надходити пізніше, ніж згадані 200 мілісекунд. У такому випадку вони будуть просто рахуватися втраченими.

Реалізація алгоритму TORA зручна для прокладки нового маршруту і кореневого обслуговування. Ключовою особливістю алгоритму TORA є його реакція на збої в системі. Він стирає недійсні маршрути, шукає нові і будує їх в одному проході розподіленого алгоритму.

Аналіз рішення для уникнення затримки в передачі

Під час передачі IP-пакетів в мережі Інтернет, інтенсивний трафік і слабке з'єднання призводить до відмов прийому пакетів в місці призначення. Щоб звести до мінімуму цю проблему, даний розділ являє собою кращу пропозицію, щоб знайти несправність лінії зв'язку, а також
відстежити дані з інших вузлів для їх відновлення.

У цьому розділі буде розглянуто два сценарії для прокладки маршруту. Це можна проілюструвати за допомогою наступної мережі. (РИС. 4.4., 4.5., 4.6.)

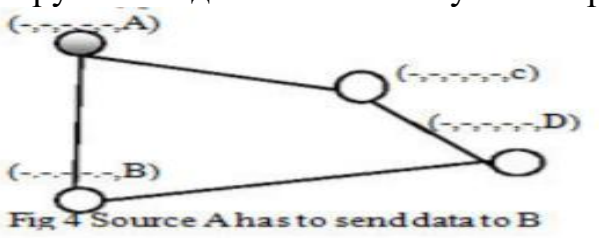

Fig 4 Source A has to send data to B

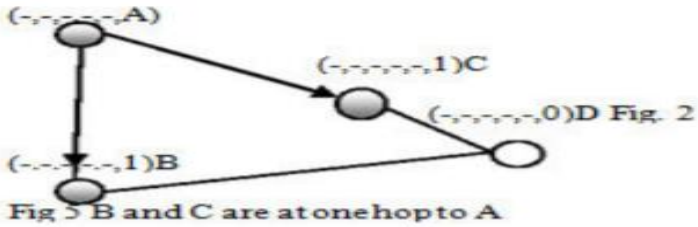

Fig. 2
Fig 5 B and C are at one hop to A

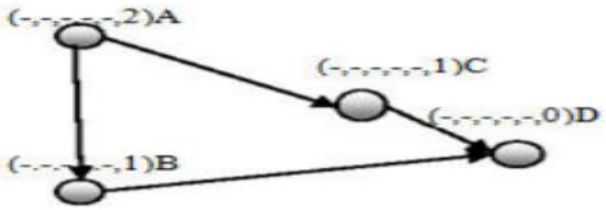

Fig.6 B and C finds D that they are at one hop

Відстеження (прокладка) маршруту

1. Вузол A повинен послати пакет вузлу D. (Рис. 4.4.)
2. A передає навколишнім хостам B і C. (Рис. 4.5.)
3. У знає, що D знаходиться в одному хопі від нього і оновлює інформаційний біт до 1. (Рис. 4.6.)
4. З так само знає, що D знаходиться в одному хопі і оновлює інформаційний біт до 1.
5. Хост A оновлює свій інформаційний біт до 2.
6. Тепер є два шляхи A-D. Один з них A-C-D, інший A-B-D. Пакет може вибрати будь-який з них.

Технічне обслуговування

1. Нехай з’єднання B-D осібно, тоді:

   • Якщо вузол уже оновлений і відокремлений, відбувається відмова у передачі пакета від A до D через вузол B.

   • Якщо вузол не оновлений і відокремлений, то інформаційний біт НЕ буде оновлюватися, отже, вузол A не знатиме про існування хоста D через B.

1. Але через існування іншого маршруту A-C-D, інформаційний біт буде оновлено.
1. Ми ставимо прапор поновлення інформаційного біта.

Використання мультиномінального розподілу

Мультиноміальний розподіл - це ймовірність розподіл результатів багаточленного експерименту. Багаточленна формула визначає ймовірність будь-який результат багаточленного експерименту. Повідомлення не може бути передано однією спробою, тому ми надсилаємо одне і те ж повідомлення, щоб усі вузли отримали повідомлення. Кількість спроб = 5. У будь-якому конкретному випробуванні ймовірність отримання повідомлення N1 дорівнює 0 або 1, N2 - 0,5, N3 - 0 або 1, N4 - 0 або 1.

p1=0.25, p2=0.25, p3=0.25, p4=0.25

P= [n! / (n1! * n2! * ... nk!)] * (p1n1 * p2n2 * . . . * (Pk*nk))

P=[5! / (1! * 2! * 1!*1!] * (0.251 * 0.252 * 0.251 * 0.251)

P=0.05859375

Це може бути реалізовано за допомогою програмування Bluetooth, J2ME Java.

4.2. Висновки до розділу

VoIP є технологією, яка забезпечує передачу голосу в мережах з пакетною комутацією протоколу IP. Час передачі залежить від пропускної здатності і прийнятих динамічних алгоритмів маршрутизації.

Досліджено причини виникнення і наслідки проблем, які виникають при використанні VoIP, а саме: латентність; зменшення потенційної можливості з деградацією QoS; зниження темпу роботи, яке може збільшити затримки, джиттер і втрати пакетів.

Розглянуто дві моделі VoIP (H.323 і SIP), і алгоритм TORA (Temporally-Ordered Routing Algorithm) для пакетної передачі даних, щоб мінімізувати затримку.

Невизначеність в передачі пакетів може бути зведена до мінімуму. Продуктивність може бути поліпшена шляхом введення FP алгоритму і ієрархічної кластеризації до його передачі.

Розділ 5. Оцінка безпеки IMS, дослідження вразливості мережі IMS.

Повна міграція на архітектуру all-IP забезпечує конвергенцію голосу, відео, даних, це велике досягнення для підтримки єдиної комунікаційної платформи для всіх комунікацій, з іншого боку, це велика проблема для забезпечення адекватної безпеки для такого неоднорідного мережевого середовища.

Безпека в телекомунікаційних мережах ніколи не була серйозною проблемою, телефонні системи характеризуються суворими правилами і суворо охороняються кінцевими вузлами. Важко отримати доступ до іншої кінцевої точки системи, якщо вас не розпізнає інший кінець. Телефонні номери даються тільки користувачам і у всіх юрисдикціях це ретельно контролюється. У той же час IMS та інтернет характеризуються широкою відкритою архітектурою, відкритими кінцевими точками, заснованими на вільно

доступному стандарті з великою кількістю загроз і вразливостей, який виходить з мережі інтернет. Завдяки цієї
нової мережевої інфраструктури інформація може бути доступна в будь-який час і в будь-якому місці, кому вона потрібна. Природно, що ці події неминуче призведуть до появи багатьох все ще невідомих вразливостей, загроз і небезпек.

Оцінка вразливості отримала важливе значення в галузі безпеки, але як і раніше відсутній аналіз вразливості в цій області, багато з існуючих методів оцінки мають обмежені можливості і не охоплюють всі області. Ціль даного розділу є обговорення поточної ситуації в галузі безпеки IMS і пропозиції методу аналізу вразливостей IMS на основі методу аналізу загроз, вразливостей і ризиків ETSI (eTVRA) і архітектури безпеки ITU-T.

У даному розділі оцінка безпеки IMS проводиться на основі двох підходів:

1. eTVRA.
2. Архітектура безпеки ITU-T. 805.

Також проводиться дослідження вразливості мережі IMS, роблячи тести з відкритим вихідним кодом IMS (ядро OpenIMS). Ідея для користувачів цього програмного забезпечення з відкритим вихідним кодом полягає в тому, щоб забезпечити розробку служб IMS та випробування концепцій навколо основних елементів IMS, які засновані на легко конфігураційному і розширювальному програмному забезпеченні (Anon, 2011). Open IMS-це експериментальне середовище для розробників і дизайнерів, що включає в себе нові концепції, парадигми і нові технології, які роблять його одним із кращих інструментів у всьому світі для тестування IMS. Цей проект популярний в Академічному та промисловому співтоваристві.

Підсистема мультимедіа IP (IMS) ключовий етап для впровадження множинних слабо з'єднаних характеристик технічного рівня і рівня обслуговування. А IMS має відкриту архітектуру, але її мережеве ядро складається з безлічі сутностей для взаємодії між різними клієнтськими пристроями.

В архітектурному проектуванні IMS використовується багаторівневий підхід, при якому транспортні та несучі служби відокремлюються від мереж сигналізації IMS і служб управління сеансами. Концепція IMS розділена на три основних рівня – рівень сервісу або програми, рівень управління чи сигналізації, а також користувальницький або транспортний рівень. Рівень додатків забезпечує інфраструктуру для розробки і управління службами. Рівень управління прокладає маршрути сигналізації, також ця область управління контролює білінговий потік інформації. Площина споживача забезпечує сердечник з доступом обладнання споживача (UE) над пересувними, Wi-Fi та широкосмуговими мережами. Організація безпеки в IMS складається з декількох частин - безпека мережевого домену (NDS), ідентифікація і аутентифікація і угода ключів (AKA). NDS забезпечує безпеку між різними вузлами в домені. NDS має справу з мережею, яка контролюється одним адміністративним органом. Домен безпеки відноситься до мережі, яка управляється один оператором мережі або забезпечує IP-безпеку між різними доменами. Аутентифікація забезпечує управління посвідченнями, якщо користувач хоче отримати доступ до мережі IMS, користувач буде аутентифікований. AKA

дозволяє організувати безпеку доступу для SIP-сервісів. Протоколи відповіді за виклик призначені для виконання ідентифікаційних тестів без спільного використання пароля між двома сторонами. Важливим компонентом безпеки IMS є IPsec, який надає послуги безпеки для: цілісності даних, аутентифікації джерела даних, захисту від anti - replay protection та деяких інших методів захисту від аналізу транспортних потоків. Доступ до мережі IMS повинен мати включені механізми безпеки і функції, такі як захищеня зв'язку користувацького обладнання. Очевидно, що важливою роллю в забезпеченні безпеки є аутентифікація кожного об'єкта в мережі.

Подібності в архітектурній структурі можуть бути знайдені між IMS і ITU-T X. 805, який є рекомендаціями MCE-T для наскрізних комунікацій. У цих рекомендаціях серії X. 800 загрози визначаються, як знищення інформації і ресурсів, пошкодження або зміну інформації, крадіжка або видалення даних, розкриття інформації та переривання роботи служб. Вони були запропоновані в якості основи для архітектури NGN для досягнення наскрізної безпеки в розподілених додатках (Atay and Masera, 2011). Це інструмент для розуміння складного набору мережевих архітектур і сервісів. X. 805 складається з 3 архітектурних частин:

– розміри безпеки, рівні безпеки і площини безпеки, як показано на РИС. 5.1.

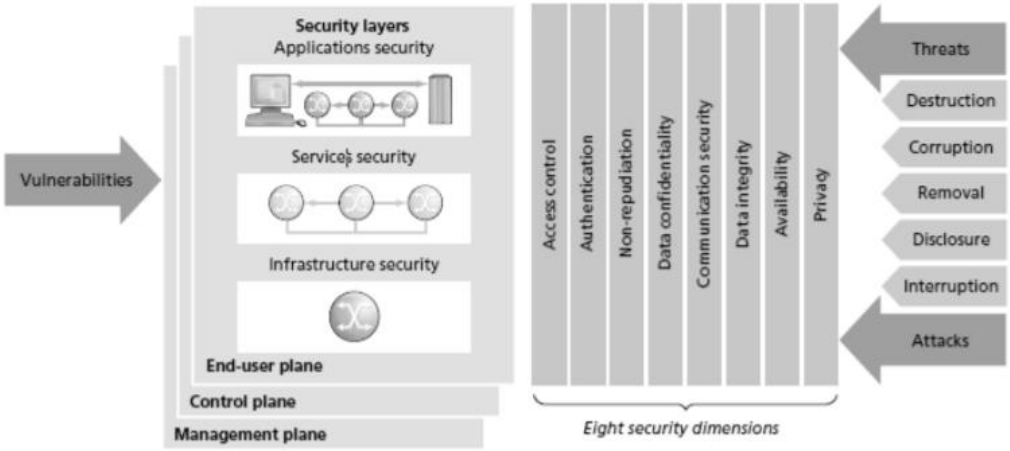

РИС. 5.1. Безпека ITU-T X. 805

Рівні безпеки також складаються з 3 – х рівнів, рівень інфраструктури, рівень безпеки сервісу, рівень безпеки сервісу, які всі разом представляють собою ієрархію угруповання обладнання і об'єктів. Але площина безпеки показують дії, які відбуваються на площині безпеки мережевого управління, площини безпеки управління і площини безпеки кінцевого користувача.

Безпека вимірювання - це методи забезпечення безпеки, спрямовані на захист: контроль доступу, аутентифікацію, відмова від анулювання, конфіденційність даних, безпека потоку зв'язку, цілісність даних, доступність та конфіденційність. Кожен рівень пов'язаний з
унікальними вразливостями, погрозами та заходами щодо їх усунення.

Одним із стандартів оцінки безпеки є стандарт ISO 15408: 2009 загальні критерії оцінки безпеки інформаційних технологій, але цей стандарт є дорогим

по часу і ресурсам. З цієї причини програма конвергенції телекомунікаційних послуг та протоколів для передових мереж (TISPAN) в Європейському інституті стандартів телекомунікацій (ETSI), найбільшої європейської організації по стандартизації телекомунікацій (Telco) з світовим впливом, розробила метод аналізу загроз, вразливостей і ризиків (eTVRA) для підтримки телекомунікаційних компаній у загальній оцінці критеріїв безпеки. eTVRA ґрунтується на CORAS (Braber et al., 2003) і структурована для забезпечення виходу, який може безпосередньо вводиться в оцінку безпеки, тим самим полегшуючи процес оцінки (Morali et al. 2009). Оцінка уразливості в eTVRA складається з 7 етапів, показаних на рис.5.2. (Morali et al., 2009). Процес починається з визначення цілей безпеки системи або системного компонента, з яких вилучаються вимоги безпеки.

Надалі складається опис активів в системі. Мета використання eTVRA полягає в тому, щоб мати можливість ідентифікувати проблеми, які існують в системі. Тому після ідентифікації активів, визначаються проблеми, загрози, які використовують ці уразливості і викликають інциденти. Вимоги безпеки і загрози розширюються у відповідності з погрозами і вразливостями. Потім проводиться аналіз і кількісна оцінка ймовірності виникнення загроз і їх впливу. Це використовується в наступному кроці для розрахунку ризику. Отже, визначені контрзаходи для обробки ризику. Цей процес застосовується ітеративно, до тих пір, поки ризик небажаних інцидентів не буде знижено до прийнятного рівня, або всякий раз, коли відбуваються зміни в навколишньому середовищі (Rosseb et al., 2006).

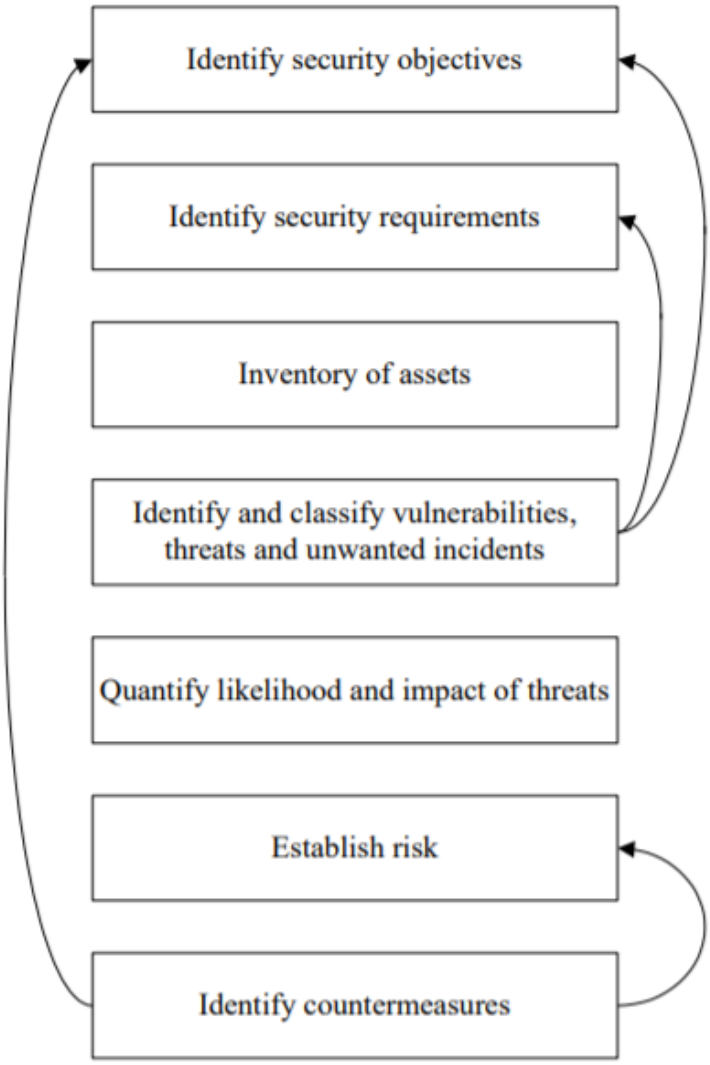

РИС. 5.2. Основні етапи роботи eTVRA.

В ході дослідження використаємо X. 805 модульні перспективи безпеки, які показані на РИС. 5.3. (Anon, 2011.) для аналізу основних вразливостей IMS, який показано з допомогою eTVRA.

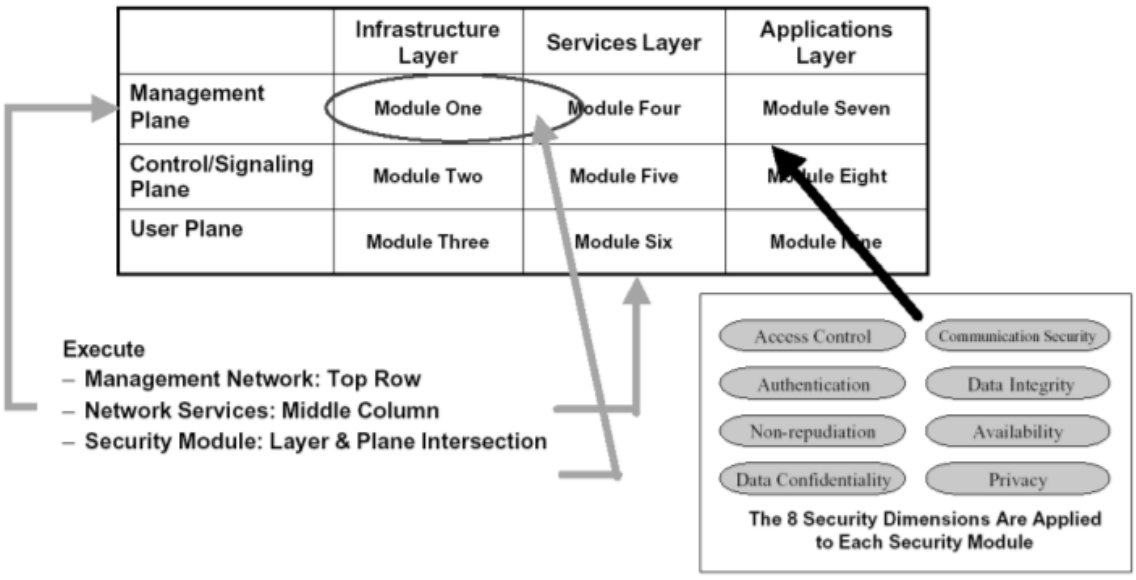

РИС. 5.3. Модульні перспективи безпеки з X. 805

Існує 9 точок зору або модулів безпеки, де необхідно ідентифікувати програмні та апаратні засоби. В кожній точці зору, в якості третього фактора в аналізі уразливості повинен бути включений людський фактор, який означає, що повинні бути оцінені всі види діяльності, а також таке рішення повинно забезпечувати не тільки аналіз вразливостей, але і кращу реалізацію та поліпшення безпеки, оскільки така модель дозволяє оновлювати безпеку при виявленні вразливостей.

Поточні стандарти безпеки IMS не охоплюють всі рішення по забезпеченню безпеки і можливості управління ризиками для основної мережі IMS. Всі рівні безпеки мають свої ризики і уразливості.

Важливо визначити апаратні і програмні компоненти IMS та їх рішення по забезпеченню безпеки, зокрема інфраструктуру і функціональну роль. 3GPP IMS та ETSI мають ряд проектів з безпеки для захисту IMS, але він все ще вразливий для декількох видів атак. ITU-T X. 805 є хорошим рішенням для забезпечення безпеки. Запропонована модель складається з восьми етапів (РИС. 5.4.), які в основному взяті з eTVRA, але деякі з кроків показані з вимірами безпеки ITU-T X. 805, рівнями і площинами. Дослідження, зроблені у пропонованій моделі, що розглядаються в наступних кроках:

- **Ідентифікація контексту / місцезнаходження** - критично важливо визначити місце розташування об'єкта в базовій мережі і його функціональний контекст з іншими об'єктами. Метою цього кроку є виявлення місця розташування абонента або точки відліку і аналіз її відносин з іншими абонентами в певному контексті.
- **Встановлення модулю** - після ідентифікації об'єкта або опорної точки необхідно проаналізувати, в якому модулі він розташований і з яким рівнем і площиною він пов'язаний. Це допоможе правильно визначити цілі забезпечення безпеки.
- **Визначення цілей і вимог безпеки** для захисту IMS від вразливостей, концепція повинна відповідати всім цілям безпеки ITU-T X. 805, але тут можуть бути винятки.
- **Інвентаризація активів** - визначення апаратних і програмних компонентів. І категоризація за
  рівнями безпеки і площин.
- **Ідентифікація та класифікація вразливостей, загроз і небажаних інцидентів** – об'єднання активів з вимірами безпеки, виявлення загроз, вразливостей і можливих небажаних інцидентів.
- **Аналіз вразливостей і небажаних інцидентів між модулями** - кожна комбінація декількох
  компонентів може включати нові ризики. Таким чином, загальна ситуація також повинна бути проаналізована. В ході дослідження було виявлено, що eTVRA не надають рекомендацій по цьому процесу.
- **Кількісна оцінка ймовірності і вплив загроз** – на цьому етапі встановлюється ризик атаки на будь-яку вразливість.
- **Ідентифікація контрзаходів** - досягнення цілей та забезпечення безпеки вимірювань.

Стандарти та протоколи постійно змінюються. IMS є досить новою архітектурою в мережах і знаходиться в процесі дослідження, вона буде змінюватись, виправлятись, розвиватись, і будуть інтегруватися нові функції. Це означає, що аналіз вразливостей повинен постійно оновлюватися і контролюватися з кожною зміною в системі.

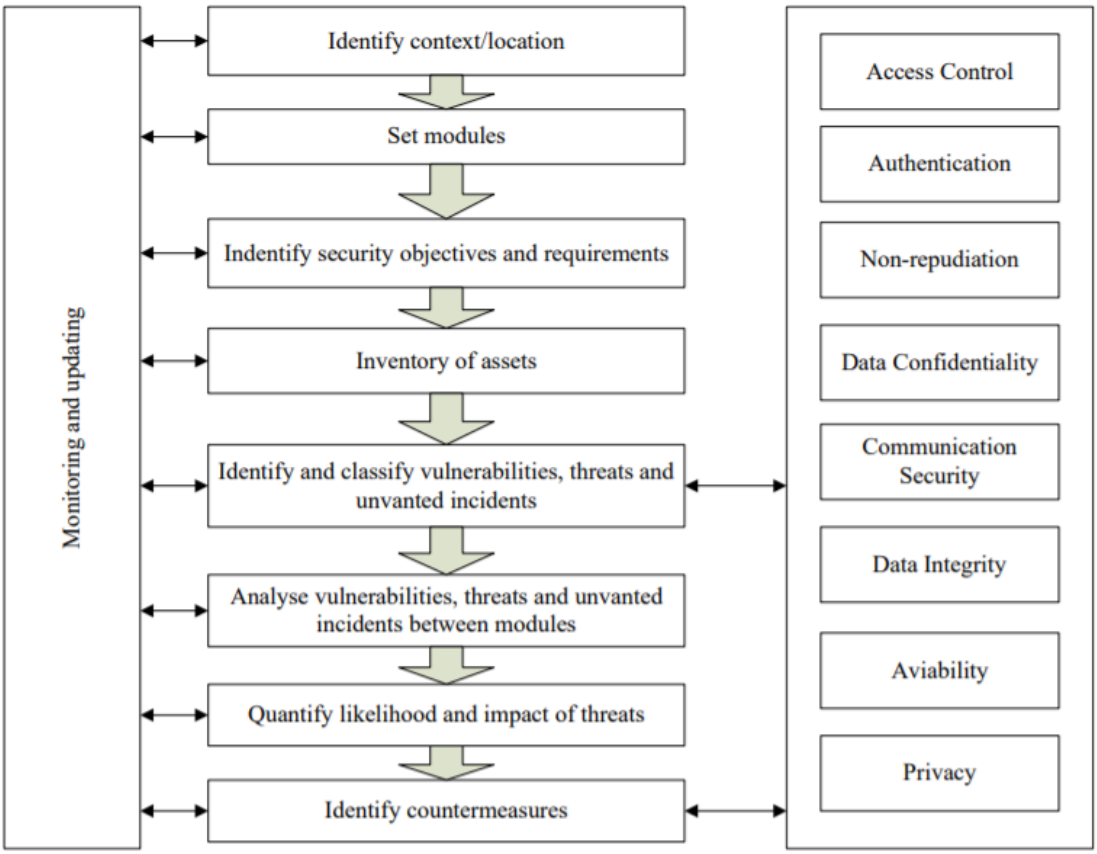

РИС. 5.4. Розширена модель тестування вразливостей IMS.

Процес дослідження показав, що не всі аспекти безпеки можуть бути адресовані кожному модулю, але в будь-якому випадку вони повинні бути проаналізовані в контексті інфраструктури та основних елементів. Будь-який об'єкт з певною функціональною цінністю в цій архітектурі може бути проаналізований як основний елемент, який повинен бути згрупований у відповідності з його конкретним рівнем безпеки і площиною, що показано в РИС. 5.5. Аналіз вразливості IMS був проведений згідно з категоризацією основних елементів.

Table 1

IMS assets by modules

	Infrastructure Layer	**Service Layer**	**Application Layer**
Management plane	CTF, CDF, CGF, PDF	Diameter (Rf, Rx, Ro) COPS (Go)	HTTP (Ut)
Control plane	CSCF, MGCF, MRFC, BGCF, IBCF, SLF, AS, DNS, ENUM	SIP/SDP(Gm, Mw, Mg, Mi, Mj,Mk, Mr), Diameter(Ch, Dx), H248 (Mp, Mn)	SIP(ISC), Diameter(Sh, Dh)
End-user plane	IM-MGW, MRFP, HSS, UE	RTP/RTCP(Mb), User profile	Voice, IM, VIDeo, State(XCAP)

Рис. 5.5. Основні елементи концепції IMS.

Аналіз вразливостей IMS показав, що IMS може піддаватися різним типам атак.

Тестування уразливості проводилося на відкритому тестовому стенді IMS. Це ядро вихідного коду проекту є відкритою частиною платформи IMS і використовується для налаштування тест-стенду для практичного моделювання сценарію.

Нижче в таблиці 2 наведено результати поточного дослідження різних вразливостей системи безпеки:

Table 2

IMS vulnerability list

Vulnerability	Weakness	Security dimension	Asset module	Impact
Message spoofing	IMS has absence of IPsec protection between user equipment and P-CSCF	Authentication	Service layer Control plane	Fraud of trust
SIP SQL injection	SIP authentication controllability is unsecure	Availability	Service layer User plane	Deniel of service
Media theft	Not enough control on media streems	Non-repudiation	Infrastructure layer Management plane	Theft of sercices
SIP flooding	Unable effectively prevent REGISTER and INVITE message flooding	Availability	Infrastructure layer Control plane	Loss of QoS for users
RTP data sniffing	No default confidentiality from data streem	Confidentiality	Application layer User plane	Theft of information
CANCEL attack	Possibility to fake SIP CANCEL request	Integrity	Service layer Control plane	Session disruption
RTP injection	RTP protocol missing media integrity protection mechanisms	Integrity	Service layer User plane	Session disruption
Man in the Middle P-CSCF attack	Authentication using SIP must be improved	Authentication	Service Layer Control plane	Impersonation of a server
Dictionary attack	Inadequate identity protection and AKA chipper algorithm use	Authentication	Application layer Control plane	Identity theft
BYE attack	Possibility to fake SIP BYE request/ not enough confidentiality protection	Integrity	Service layer Control plane	Disruption of session
DNS Cache Poisoning	Not enough connection integrity protection	Integrity	Infrastructure plane Control plane	Loss of service
Network topology disclosure	Not protected SIP messages	Confidentiality	Infrastructure layer Control plane	Leak of network topology
HTTP Parse Attack	Improperly data ContentLenght regulation	Availability	Infrastructure layer Control plane	Loss of services
User equipment configuration tampering	Probability lack of user education in security questions	Availability	Infrastructure layer Control plane	Denial of services

Оцінка потенційних загроз і вразливостей повинна бути повторена в обов'язковому порядку, тому її необхідно відстежувати і оновлювати. Більшість заходів безпеки виявляються стандартними механізмами, такими як IPSec і TLS або аутентифікація і авторизація. Але такі атаки, як SQL-запити, не можуть бути захищені і вимагають додаткового інструменту реалізації найбільш ефективного

захисту, метод захисту повинен мати інструмент виявлення і запобігання вторгнень. Це допомогло б покращити захист від загроз пов'язаних з людським фактором.

5.2. Висновки до розділу.

У даному розділі розглянуто реалізацію моделі eTVRA в аналізі вразливостей IMS, яка доповнюється рекомендаціями ITU-T X. 805 безпеки. Пропонується метод для повного покриття тестування вразливостей. Загрози та вразливості ядра IMS були зроблені на відкритому випробувальному стенді IMS в Focus Fraunhofer. Одним з основних протоколів, який стикається з багатьма вразливостями, є протокол SIP. У розділі були показані основні загрози і майбутня кількісна оцінка вразливостей, якій був зроблений аналіз. Також як перспективна технологія для захисту може бути впровадження системи виявлення та запобігання вторгнень. Дослідження показують, що найбільша вразливість пов'язана з рівнем додатків і площиною управління, що означає, що цим частинам потрібно приділяти додаткову увагу для захисту.

ВИСНОВКИ

У ході аналізу концепції розвитку телекомунікаційних мереж було досліджено багаторівневу архітектуру NGN, яка була предтечею мережі IMS. Перехід на IMS дає появу персоналізованих послуг, заснованих на передачі мови, тексту, графіки і відео в будь-якій комбінації, створення нових сервісів, а також об'єднання та вдосконалення існуючих. Дослідження функцій і архітектури Softswitch дає зрозуміти, що схожість Softswitch і IMS полягає в наступному, обидві архітектури майже ідентичні, в обох ідея надання всіх послуг на базі IP-мережі, поділ функцій управління викликом і комутації. В них є дуже багато спільного і в той же час концепції сильно відрізняються. CSCF в IMS розділено на три підфункції: P-CSCF, I-CSCF, S-CSCF. Якщо розбирати зміст кожної функції тоді помітні значні відмінності Softswitch і IMS.

Об’єднати декілька мереж ми не можемо, тому що потужності софтсвіча не вистачить, щоб подолати таке навантаження. Виходячи з цього, можна зробити висновок, що S-CSCF, P-CSCF, I-CSCF – це окремі софтсвічі. Перевага і відмінність концепції IMS полягає в тому, що вона надає доступу до мультисервісних послуг будь-якому кінцевому абоненту (телефон, комп’ютер, стаціонарний телефон) за допомогою різних мереж доступу. IMS забезпечує взаємодію з зовнішніми мережами традиційної телефонії як для фіксованої, так і для мобільного зв'язку. Наявність універсального технологічного середовища забезпечує інтеграцію різних комунікаційних додатків. У розділі 2 розглянуті основні елементи архітектури і функції, за принципом яких досягається можливість для вирішення таких завдань: як реалізація декількох послуг в рамках одного сеансу зв'язку; встановлення великого числа сеансів зв'язку, причому беруть участь в цих сеансах абоненти які можуть використовувати різні пристрої доступу. Абонентам пропонуються різного роду послуги, доставка яких ґрунтується на загальному підході. Для операторів зв’язку перехід на LTE є доцільним з економічної точки зору, тому що: 1) зростає надійність мережі; 2) зменшується вартість передачі одиниці трафіку.

VoIP є технологією, яка забезпечує передачу голосу в мережах з пакетною комутацією протоколу IP. Час передачі залежить від пропускної здатності і прийнятих динамічних алгоритмів маршрутизації.

Досліджено причини виникнення проблем і їх наслідки, які виникають при використанні VoIP, а саме: латентність; зменшення потенційної можливості з деградацією QoS; зниження темпу роботи, яке може збільшити затримки, джиттер і втрати пакетів.

Розглянуто дві моделі VoIP (H.323 і SIP), і алгоритм TORA (Temporally-Ordered Routing Algorithm) для пакетної передачі даних, щоб мінімізувати затримку.

Невизначеність в передачі пакетів може бути зведена до мінімуму. Продуктивність може бути поліпшена шляхом введення FP алгоритму і ієрархічної кластеризації до його передачі.

У розділі 5 було розглянуто реалізацію моделі eTVRA в аналізі вразливостей IMS, яка доповнюється рекомендаціями ITU-T X. 805 безпеки.

Пропонується метод для повного покриття тестування вразливостей. Загрози та вразливості ядра IMS були зроблені на відкритому випробувальному стенді IMS в Focus Fraunhofer. Одним з основних протоколів, який стикається з багатьма вразливостями, є протокол SIP. У розділі були показані основні загрози і майбутня кількісна оцінка вразливостей, якій був зроблений аналіз. Також як перспективна технологія для захисту може бути впровадження системи виявлення та запобігання вторгнень. Дослідження показують, що найбільша вразливість пов'язана з рівнем додатків і площиною управління, що означає, що цим частинам потрібно приділяти додаткову увагу для захисту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] Гольдштейн Б.С. SOFTSWITCH / Гольдштейн Б.С., Гольдштейн А.Б.. – СПб: БХВ-Петербург., 2014. – 368 с.

[2] Константин Самуйлов. Сети и телекоммуникации. Учебник и практикум для СПО / Константин Самуйлов, Валерий Василевский, Анна Королькова. – Москва: Юрайт, 2019. – 363 с. – (Профессиональное образование).

[3] IMS (электросвязь) [Електронний ресурс] – Режим доступу до ресурсу: https://ru.wikipedia.org/wiki/IMS_(%D1%8D%D0%BB%D0%B5%D0%BA%D1%82%D1%80%D0%BE%D1%81%D0%B2%D1%8F%D0%B7%D1%8C).

[4] IP Multimedia Subsystem - IP Multimedia Subsystem [Електронний ресурс] – Режим доступу до ресурсу: https://ru.qwe.wiki/wiki/IP_Multimedia_Subsystem#Charging.

[5] IP Multimedia Subsystem (IMS) Handbook / Ahson S.A., Ilyas M.., 2009. – 562 с.

[6] Developing SIP and IP Multimedia Subsystem (IMS) Applications.. – 690 с.

[7] F. Galán. Design and Implementation of an IP Multimedia Subsystem (IMS) Emulator Using Virtualization Techniques : дис. канд. техн. наук / F. Galán.. – 12 с.

[4] СЕТИ NGN. ОБОРУДОВАНИЕ IMS / Б.С. Гольдштейн, В.Ю. Гойхман, Н.Г. Сибирякова, Ю.В. Столповская. – СПб: Теледом, 2010. – 56 с.

[8 Next Generation Network (NGN) peculiarities Part 1 [Електронний ресурс] – Режим доступу до ресурсу: http://lib.tssonline.ru/articles2/fix-op/osobennosti-setey-novogo-pokoleniya-(ngn).-chast-1.-next-generation-network-(ngn)-peculiarities.-part-1.

[9] Подводная часть айсберга по имени NGN [Електронний ресурс] – Режим доступу до ресурсу: http://tssonline.ru/articles2/fix-op/podvodn_chast_iceberg_imeni_ngn_chapt_2.

[10] IMS [Електронний ресурс] – Режим доступу до ресурсу: https://www.intuit.ru/studies/courses/1150/157/lecture/28726?page=4.

[11] IP Multimedia Subsystem - универсальная архитектура для услуг [Електронний ресурс] – Режим доступу до ресурсу: http://citcity.ru/13853/.

[12] Дополнительные услуги в сетях IMS [Електронний ресурс] – Режим доступу до ресурсу: https://helpiks.org/6-66895.html.

[4] Д. Ю. Пономарев. ИССЛЕДОВАНИЕ ВОЗМОЖНОСТЕЙ ИМИТАЦИОННОГО МОДЕЛИРОВАНИЯ ПРОЦЕССОВ ОБРАБОТКИ СИГНАЛЬНЫХ ПОТОКОВ В СЕТИ IMS : дис. канд. техн. наук / Д. Ю. Пономарев. – Красноярск, 2009. – 5 с.

[13] NAURIS PAULINS, PETERIS RIVZA. VULNERABILITY ANALYSIS OF IP MULTIMEDIA SUBSYSTEM (IMS) : дис. канд. техн. наук / . – Latvia. – 8 с.

[14] Lalitha R.V.S. Voice over Internet Protocol (VoIP) Performance Analysis, QoS Measures to Minimize Packet Loss, and Identifying Link Failures during Transmission : дис. канд. техн. наук / Lalitha R.V.S., 2013. – 6 с.

[15] Журнал научных и прикладных исследований. // Научно-практический журнал №4. – 2016. – №1. – С. 172.

[16] Measuring the Performance of VoIP over Wireless LAN / . – Kentucky. – 6 с.

[17] Harilaos Koumaras. ADAMANTIUM PROJECT: ENHANCING IMS WITH A PQoS-AWARE MULTIMEDIA CONTENT MANAGEMENT SYSTEM : дис. канд. / Harilaos Koumaras. – France, 2008. – 9 с.

[18] Evolution from Fixed Softswitch to IMS [Електронний ресурс] – Режим доступу до ресурсу: https://www.zte.com.cn/global/about/magazine/zte-communications/2007/2/en_25/162452.html.

[19] Недостатки NGN [Електронний ресурс] – Режим доступу до ресурсу: https://studbooks.net/2354253/tehnika/nedostatki.