НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Інститут телекомунікаційних систем

Кафедра Інформаційно-телекомунікаційних мереж

До захисту допущено:

Завідувач кафедри

_____ Лариса ГЛОБА

«___»_____2020 р.

Дипломна робота

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Інформаційно-комунікаційні технології»

спеціальності 172 «Телекомунікації та радіотехніка»

на тему: «Забезпечення безпеки в мережах IP-телефонії »

Виконав:
студент IV курсу, групи ТІ-61
Сачук Денис Володимирович _____

Керівник:
доцент кафедри ІТМ ІТС, к.т.н., доцент
Правило Валерій Володимирович _____

Рецензент:
доцент кафедри ТК ІТС, к.т.н., доцент
Явіся Валерій Сергійович _____

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

Київ – 2020 року

Національний технічний університет України
«Київський політехнічний інститут імені Ігоря Сікорського»
Інститут телекомунікаційних систем
Кафедра Інформаційно-телекомунікаційних мереж

Рівень вищої освіти – перший (бакалаврський)

Спеціальність – 172 «Телекомунікації та радіотехніка»

Освітньо-професійна програма «Інформаційно-комунікаційні технології»

ЗАТВЕРДЖУЮ
Завідувач кафедри
_____ Лариса ГЛОБА
«___»_____2020 р.

ЗАВДАННЯ
на дипломну роботу студенту
Денису САЧУКУ

1. Тема роботи «Забезпечення безпеки в мережах IP-телефонії», керівник роботи доцент кафедри інформаційно-телекомунікаційних мереж ІТС Правило Валерій Володимирович, к.т.н., доцент, затверджені наказом по університету від «30» березня 2020 р. № 924-с

2. Термін подання студентом роботи 8 червня 2020 р.

3. Вихідні дані до роботи обраний більш безпечний протокол аутентифікації.

4. Зміст роботи

1. Розглянути різні архітектури мереж IP-телефонії,можливі засоби забеспечення безпеки та запобігання загроз.
2. Проаналізувати принципові відмінності архітектур мереж з використанням серверів AAA, та протоколів TACACS+ та RADIUS.
3. Виходячи з аналізу та порівняння, запропунувати кращу технологію автентифікації для забезпечення безпеки в мережі IP-телефонії.

5. Перелік ілюстративного матеріалу (із зазначенням плакатів, презентацій тощо)

1. Тема, актуальніст, мета, задачі
2. Аналіз архітерктури мережі IP-телефонії
3. Аналіз можливих загроз методів їх подолання
4. Порівняння протоколів автентифікації
5. Висновки

6. Дата видачі завдання 14 листопада 2019

Календарний план

№ з/п	Назва етапів виконання дипломної роботи	Термін виконання етапів роботи	Примітка
1	Уточнення постановки задачі	16.11.2019 – 19.11.2019	виконано
2	Аналіз літератури	17.12.2019 – 22.01.2020	виконано
3	Обгрунтування вибору рішення	22.02.2020 – 25.02.2020	виконано
4	Аналіз даних та їх класифікація	26.03.2020 – 27.04.2020	виконано
5	Розгляд архітектури мережі	27.04.2020 – 30.04.2020	виконано
6	Ознайомлення з методами забезпечення безпеки	01.05.2020 – 02.05.2020	виконано
7	Розгляд недоліків безпеки IP-мережі	02.05.2020 – 03.05.2020	виконано
8	Дослідження протоколів автентифікації	03.05.2020 – 05.05.2020	виконано
9	Порівняння протоколів за показником безпеки	05.05.2020 – 06.06.2020	виконано

Студент Денис САЧУК

Керівник Валерій ПРАВИЛО

РЕФЕРАТ

Робота містить 76 сторінок, 19 рисунків та 2 таблиці. Було використано 8 джерел.

Мета роботи: розглянути різні архітектури мереж IP-телефонії,можливі засоби забеспечення безпеки та запобігання загроз. Розглянути протоколи автентифікації і на основі аналізу їх подібності та відмінності виявити протокол з найбільшою стійкістю до дешефрування та несанкціонованої автентифікації.

Проведено огляд основних методів забезпечення безпеки в мережах IP-телефонії:

1. Використання технологій автентифікації.
2. Використання методів криптографічного захисту.
3. Використання захисту від прослуховування.

Розглянуто різноманітність використання пристроїв, можливі схеми їх підключення, проведено оцінювання та аналіз стійкості пристроїв. Методом оцінювання було виявлено набільш стійкі протокли шифрування та дешифрування, їх використання з різноманітними пристроями.

Проаналізовано принципові відмінності архітектур мереж з використанням серверів AAA, таких як TACACS+ та RADIUS. Запропоновано використання протоколу TACACS+.

ABSTRACT

The work contains 76 pages, 19 figures and 2 tables. 8 sources were used.

Purpose: to consider different architectures of IP-telephony networks, possible means of security and threat prevention. Consider authentication protocols and, based on the analysis of their similarities and differences, identify the protocol with the greatest resistance to bargaining and unauthorized authentication.

An overview of the main methods of security in IP-telephony networks:

1. Use of authentication technologies.

2. Use of cryptographic protection methods.

3. Use eavesdropping protection.

The variety of use of devices, possible schemes of their connection are considered, the estimation and the analysis of stability of devices is carried out. The evaluation method revealed the most stable encryption and decryption protocols, their use with various devices.

The fundamental differences of network architectures using AAA servers such as TACACS + and RADIUS are analyzed. The use of the TACACS + protocol is proposed.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

VoIP	-	Voice over IP
IP	-	Internet Protocol
DoS	-	Denial of Service
ATM	-	Asynchronous Transfer Mode
ISDN	-	Integrated Services Digital Network
ADSL	-	Asymmetric Digital Subscriber Line
RTP	-	Real-time Transport Protocol
UDP	-	User Datagram Protocol
TCP	-	Transmission Control Protocol
ITU-T	-	International Telecommunication Union
RIP	-	Routing Information Protocol
IGRP	-	Interior Gateway Routing Protocol
EIGRP	-	Enhanced Interior Gateway Routing Protocol
IS-IS	-	Intermediate System-to-intermediate System
OSPF	-	Open Shortest Path First
BGP	-	Border Gateway Protocol
SIP	-	Session Initiation Protocol
IPDC	-	Internet Protocol Device Control
SGCP	-	Simple Gateway Control Protocol
MGCP	-	Media Gateway Control Protocol
AAL5	-	ATM Adaptation Layer 5
IPX	-	internetwork packet exchange
SDP	-	Session Description Protocol
UA	-	User Agent
UAC	-	User Agent Client
UAS	-	User Agent Server
RSVP	-	Resource ReSerVation Protocol
RTSP	-	Real Time Streaming Protocol

SDP	-	Session Description Protocol
DES	-	Data Encryption Standard
IDEA	-	International Data Encryption Algorithm
ECB	-	Electronic codebook
CBC	-	Cipher block chaining
OFB	-	Output feedback
SHA	-	Secure Hash Algorithm
MD4	-	Message Digest 4
AAA	-	Authentication Authorization and Accounting
PPP	-	Point-to-Point Protocol
PAP	-	Password Authentication Protocol
CHAP	-	Challenge Handshake Authentication Protocol
RADIUS	-	Remote Access Dial-In User Service
TACACS	-	Terminal Access Controller Access Control System

ВСТУП

Актуальність. У сучасному світі безпека мережі є критичною. Підприємствам необхідно забезпечити безпечний доступ працівників до мережевих ресурсів у будь-який час, для чого сучасна стратегія безпеки мережі повинна враховувати ряд факторів, таких як підвищення надійності мережі, ефективне управління безпекою та захист від постійних загроз та нових методів атаки.

Мета роботи. Метою роботи є пошук можливостей забезпечення безпеки в IP-телефонії за допомогою наявних протоколів автентифікації, та виявлення найкращого протколу по показникам захисту з вже існуючих.

Для досягнення мети дослідження було поставлено та вирішено такіосновні задачі:

1. Проаналізувати різні архітуктури мереж IP-телефонії.
2. Проналізувати сучасні методи забезпечення безпеки.
3. Виявити кращі методи автентифікації для захисту мережі.
4. Порівняти протокои автентифікації по критерію безпеки.

Об’єкт дослідження – сучасні мережі VoIP та IP-телефоніїї.

Предмет дослідження – протоколи непрямої автентифікації TACACS+ та RADIUS.

IP-телефонія проникає все глибше в наше життя. Але що це - технологія, послуга чи напрямок?

Термін IP телефонія з’явився не так давно. Це буквально означає «телефонія із засобом передачі через IP». Оскільки протокол IP використовується для роботи глобальної мережі Інтернет, то IP-телефонія часто асоціюється саме з Інтернетом. З одного боку, IP-телефонія безпосередньо завдячує своєю популярністю Інтернету, з іншого боку, Інтернет при її використанні відіграє лише роль транспорту. При цьому IP-телефонія не обмежується Інтернетом і може працювати через будь-які мережі на основі протоколу IP.

Тому в широкому розумінні термін IP-телефонія повинен поширюватися не тільки на Інтернет, але й на корпоративні мережі. Далі, для позначення IP-телефонії буде використано більш стандартну абревіатуру VoIP (Voice over IP), яка більш точно описує суть явища та усуває деякі розбіжності при порівнянні звичайної телефонії та IP.

Якщо говорити про недоліки та вразливості IP-телефонії, то спочатку слід зазначити ті самі проблеми, від яких страждають інші служби, що використовують протокол IP. Це схильність до вірусів, DoS-атак, несанкціонованому віддаленому доступу тощо. Незважаючи на те, що при створенні інфраструктури IP-телефонії ця служба зазвичай відокремлена від мережевих сегментів, в яких передаються не голосові дані, це все рівно не є гарантією безпеки. Сьогодні велика кількість компаній інтегрує IP-телефонію з іншими програмами, такими як електронна пошта. З одного боку, таким чином з'являються додаткові зручності, а з іншого - нові вразливості.

Крім того, для роботи мережі IP-телефонії потрібна велика кількість компонентів, таких як сервери підтримки, комутатори, маршрутизатори, брандмауэры, IP-телефони тощо.

Серед основних загроз мережі IP-телефонії:

- реєстрація чужого терміналу, що дозволяє телефонувати за чужий рахунок;
- внесення змін у голосовий або сигнальний трафік;
- зниження якості голосового трафіку;
- перенаправлення голосового або сигнального трафіку;
- перехоплення голосового або сигнального трафіку;
- підроблені голосові повідомлення;
- закінчення сеансу спілкування;
- відмова в обслуговуванні;

- віддалений несанкціонований доступ до компонентів інфраструктури IP-телефонії;
- несанкціоноване оновлення програмного забезпечення на IP-телефоні (наприклад, з метою впровадження трояну чи шпигунських програм);
- хакерська система виставлення рахунків (для телефонії оператора).

Це не весь перелік можливих проблем, пов’язаних із використанням IP-телефонії. Альянс безпеки VoIP (VOIPSA) розробив документ, що описує широкий спектр загроз IP-телефонії, який, крім технічних загроз, включає вимагання через IP-телефонію, спам тощо.

Тим не менш, головна вразливість IP-телефонії - це людський фактор. Проблема безпеки при розгортанні IP-телефонної мережі часто відступає на другий план, і рішення приймається без участі експертів із безпеки. Крім того, фахівці не завжди правильно приймають рішення, навіть якщо в ньому присутні відповідні захисні механізми або придбано обладнання безпеки, яке не призначене для ефективної обробки голосового трафіку (наприклад, брандмауери можуть не розуміти захищений протокол сигналізації, який використовується у IP-телефонії) Зрештою, організація змушена витрачати додаткові фінансові та кадрові ресурси на захист розгорнутого рішення або миритися з його незахищеністю.

РОЗДІЛ 1

АНАЛІЗ АРХІТЕТКУР IP-ТЕЛЕФОНІЇ

1. Побудова мережі IP-телефонії

Мережа IP-телефонії - це комбінація кінцевого обладнання, каналів зв'язку та вузлів комутації. Мережі IP-телефонії побудовані за тим же принципом, що і Інтернет. Однак, на відміну від Інтернету, мережі IP-телефонії мають особливі вимоги щодо забезпечення якості передачі голосу. Одним із способів скорочення часу затримки голосових пакетів у вузлах комутації є зменшення кількості вузлів комутації, що беруть участь у з'єднанні. Тому при побудові великих транспортних мереж спочатку організовується магістраль, яка забезпечує проїзд трафіку між окремими ділянками мережі, а кінцеве обладнання (шлюзи) включається в найближчий вузол комутації. Оптимізація маршруту може покращити якість наданих послуг. Коли інші оператори підключені до мережі, їх обладнання також підключено до найближчого комутаційного вузла.

Для зв'язку між пристроями всередині мережі та з пристроями інших мереж IP-телефонії використовуються виділені канали або Інтернет. До речі, термінальні пристрої спілкуються між собою, мережі IP-телефонії можна розділити на виділені, інтегровані та змішані.

У виділених мережах на Рис. 1.1 зв’язок між термінальними пристроями здійснюється через виділені канали, а смуга пропускання цих каналів використовується лише для передачі голосових пакетів. Найчастіше провайдери IP-телефонії не будують власну мережеву інфраструктуру, а орендують канали у первинних мережевих провайдерів. Це дозволяє знизити витрати на експлуатацію мережі та збільшити рентабельність інвестицій.

Основна перевага виділеної мережі - висока якість передачі голосу, оскільки такі мережі призначені лише для передачі голосового трафіку. Крім того, для забезпечення гарантованої якості послуг, що надаються в цих

мережах, крім протоколу IP використовуються й інші транспортні протоколи: ATM та Frame Relay.

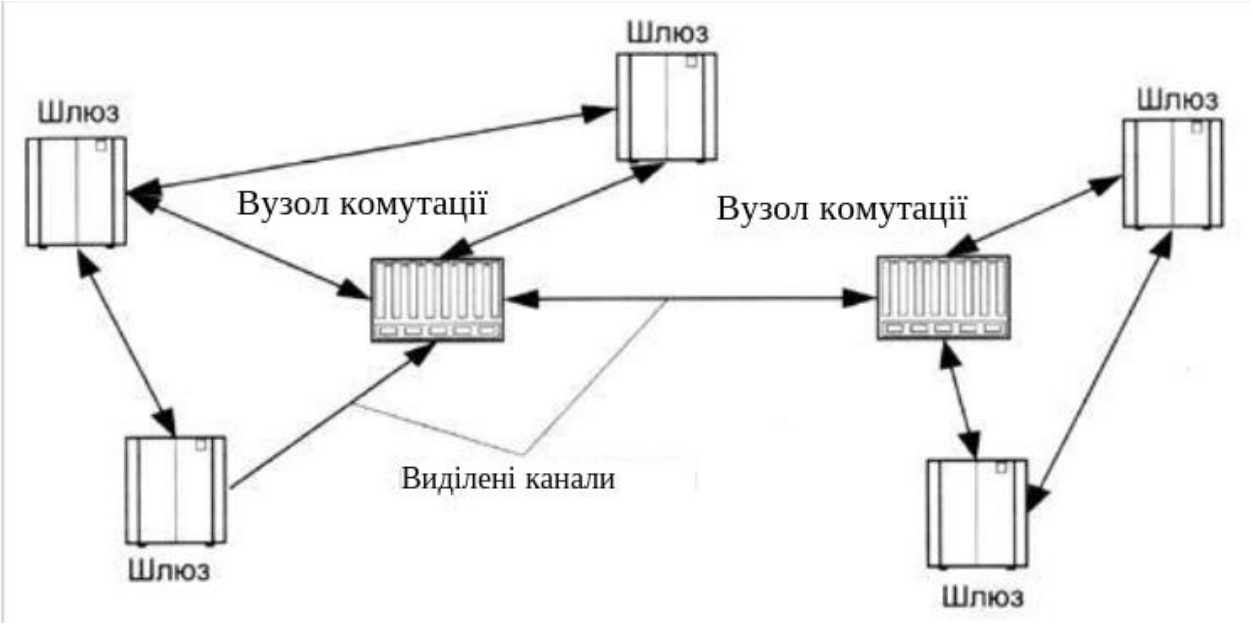

Рис. 1.1. Структурна схема виділеної мережі

У інтегрованих мережах на Рис. 1.2 IP-телефонії глобальний Інтернет використовується для зв'язку між пристроями. Це може бути існуюча власна мережа або доступ до Інтернету через провайдерів. Якщо оператор має власну мережу Інтернет, то для надання послуг IP-телефонії він встановлює лише додаткове обладнання, яке перетворює мовлення в дані і навпаки, та модернізує існуюче обладнання для забезпечення якості наданих послуг.

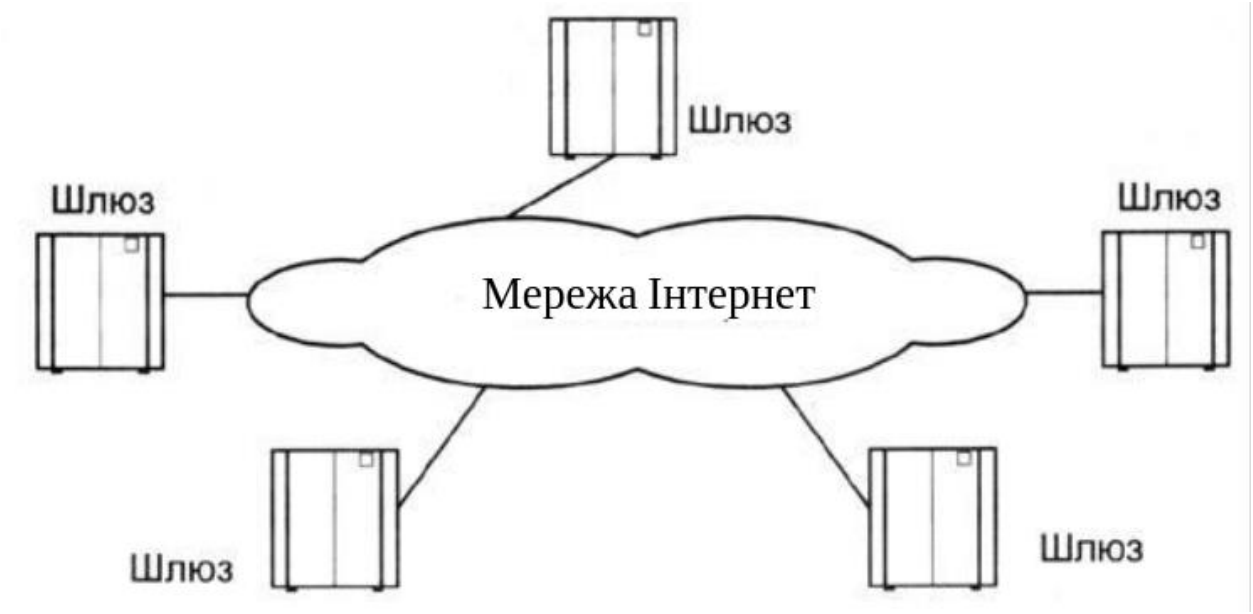

Рис. 1.2. Структурна схема інтегрованої мережі

Якщо оператор IP-телефонії використовує послуги Інтернет-провайдерів, якість послуг такої мережі може бути низькою, оскільки звичайні мережі Інтернет не призначені для передачі інформації в режимі реального часу.

З різних причин оператори мережі IP-телефонії можуть використовувати спеціальні канали та Інтернет для підключення своїх пристроїв у мережі. Такі мережі можна назвати мережами змішаного типу, Рис 1.3.

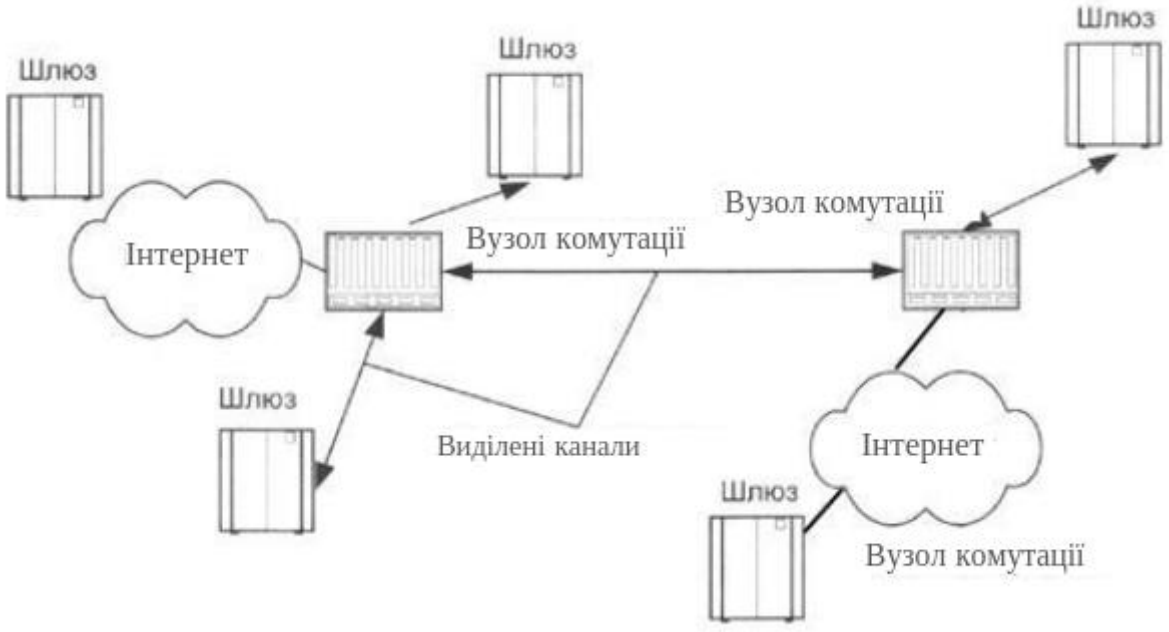

Рис. 1.3. Структурна схема змішаної мережі

Питання, які канали використовувати для зв'язку між пристроями, вирішує оператор індивідуально, залежно від можливостей.

1.1. Механізм роботи

Щоб зрозуміти механізм VoIP на Рис. 1.4 і телефонії загалом, потрібно зрозуміти, як працює звичайний телефон. І це працює так: ваш голос приймається мікрофоном, який випромінює електричний сигнал, що відповідає вашому голосу. Цей сигнал подається на лінію, передається по ній і доходить до телефону вашого співрозмовника. Там він подається на динамік, вбудований у слухавку, і відтворюється у вусі співрозмовника. Аналогічна схема працює з боку другого учасника розмови - його голос передається у вашу трубку.

Це схема для двох телефонів, коли їх багато, між ними встановлюється комутаційне обладнання - автоматична станція, яка знає, на якому порту - який абонент, і перемикає абонента на потрібну лінію. Рядок у цьому випадку відображається на цифровий номер - саме той, який повинен набрати абонент котрий робить виклик, щоб дістатися до іншого абонента.

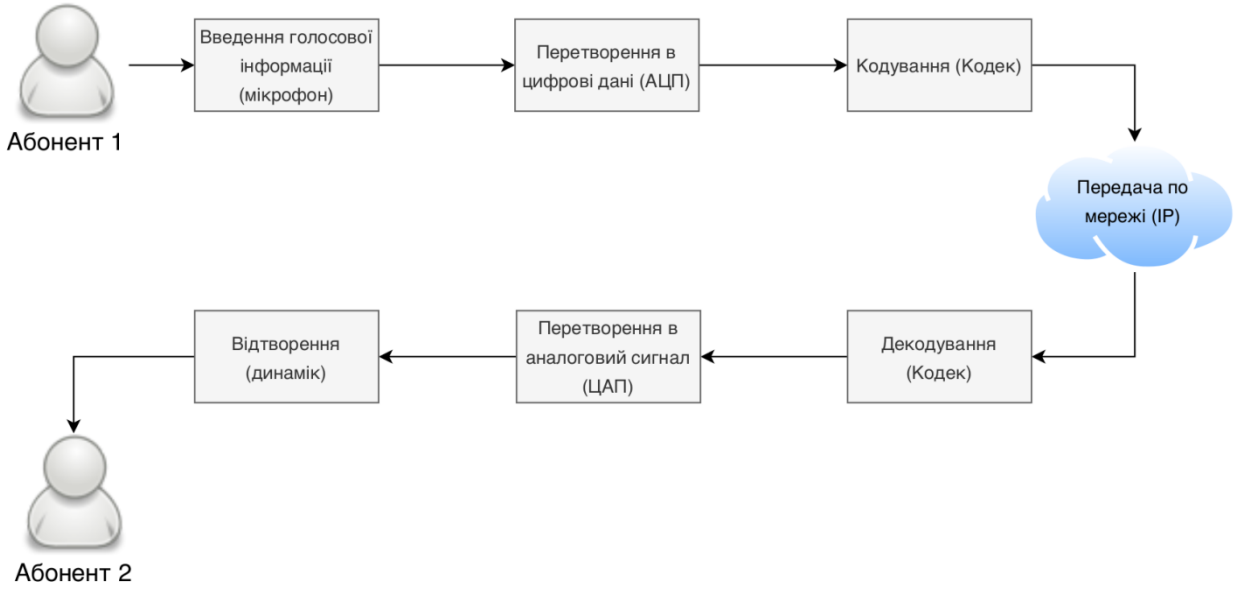

Рис. 1.4. Механізм передачі голосу в мережі

Відповідно, в зв'язку беруть участь 3 точки: абонент 1, абонент 2 і точка реєстрації абонентів. У звичайної телефонії абоненти - це телефонні апарати, а точка реєстрації - АТС. Тут важливо відзначити, що в чисто цифрових системах, наприклад, в ISDN, для набору номера не використовуються навіть тональний сигнал: коли абонент 1 набирає номер абонента 2, то цей номер передається на АТС в цифровому вигляді. Для цього в технології ISDN є спеціальний канал для управління з'єднаннями - т.зв. D-канал. Якщо згадати про ISDN докладніше, то абонентське підключення є формулою 2B + D. 2B - це два B-каналу пропускною спроможністю по 64 Кбіт за сек. кожен, а D-канал має пропускну здатність 16 Кбіт за сек. Причому канали ці є віртуальними - їх сигнали передаються по одному дроту, а поділ смуги, яка в сумі становить 144 Кбіт за сек., здійснюється методом мультиплексування.

Також на її основі ISDN досить просто зрозуміти, як працює VoIP, адже ISDN, являлася першою повністю цифровою масовою системою зв'язку, стала прообразом VoIP. Так ось, ISDN-абонент має 2 B-канали, кожен з яких може передавати голос, факс або дані. Швидкість 64 кбіт в сек. була обрана не випадково - саме така смуга потрібно кодеку, який з мінімальними втратами може передавати голос. Можна помітити, що 64 кбіт в секунду це, взагалі-то,

забагато для одного голосового з'єднання. Але не будемо забувати, що за часів розробки ISDN швидкість аналогових модемів складала 14.4 кбіт в сек., а технологій ADSL і VoIP взагалі не існувало. Відповідно, телефоністам не було великого сенсу економити на пропускній здатності, ускладнюючи ISDN-телефони. Більш того, швидкість підключення до Інтернет - 64 кбіт за сек, яку забезпечував ISDN, була в той час дуже і дуже високою.

Повернемося до телефонії. При роботі ISDN як голосового зв'язку використовується 2 канали: B-канал (64 кбіт в сек.) Для передачі голосу і D-канал (16 кбіт в сек.) Для т.зв. сигналізації, тобто управління установкою і обслуговуванням з'єднання. Саме принцип поділу голосового трафіку і сигналізації є однією з ознак чисто цифрових систем. Аналогові системи змушені керувати з'єднанням по тому ж каналу.

Поділ управління викликом і голосового трафіку зберігається і в VoIP. Взагалі, VoIP, по суті своїй, дуже схожий з ISDN: та ж повністю цифровий зв'язок, наявність спеціальних абонентських терміналів. Ось тільки середовище передачі - протокол IP.

1.2. Топологія мережі

У рішень для роботи в Інтернет, як правило, дві основні топології - "з сервером" і "клієнт-клієнт". У топології з сервером, абоненти підключаються до нього і передають усі дані тільки через сервер, рис 1.5. При використанні топології клієнт-клієнт, абоненти можуть безпосередньо обмінюватися даними. Існує і третя, гібридна, топологія - коли використовується топологія клієнт-клієнт, але при цьому, задіяний і сервер, але не для обміну всією інформацією, а тільки для реєстрації та пошуку абонента для виклику.

Рис. 1.5. Топологія мережі з сервером

Топологія з використанням сервера, як правило, використовується в тому випадку, якщо абоненти перебувають за міжмережевими екранами(фаєрволом) або трансляцією адрес. У цьому випадку вони часто не можуть обмінюватися пакетами безпосередньо, оскільки вхідні з'єднання блокуються фаєрволом. У цій топології абоненти повністю здійснюють обмін через сервер.

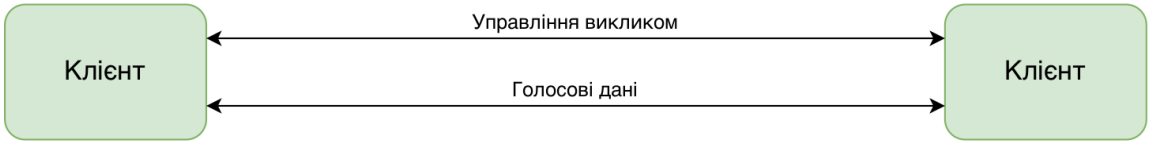

Рис. 1.6. Топологія мережі клієнт-клієнт

Топологія "клієнт-клієнт" на рис 1.6. використовується, як правило, коли клієнти можуть обмінюватися пакетами безпосередньо один з одним. Це найефективніша топологія для VoIP, оскільки відсутня необхідність утримання постійного сервера і каналів зв'язку до нього. Адже кожен VoIP-розмова може займати смугу пропускання від 32 до 160 Кбіт в сек., І якщо помножити цю цифру на кількість одночасних розмов, то може вийти дуже велике значення. Однак у такій топології можуть виникнути складнощі з визначенням IP-адреси, на котру потрібно дзвонити.

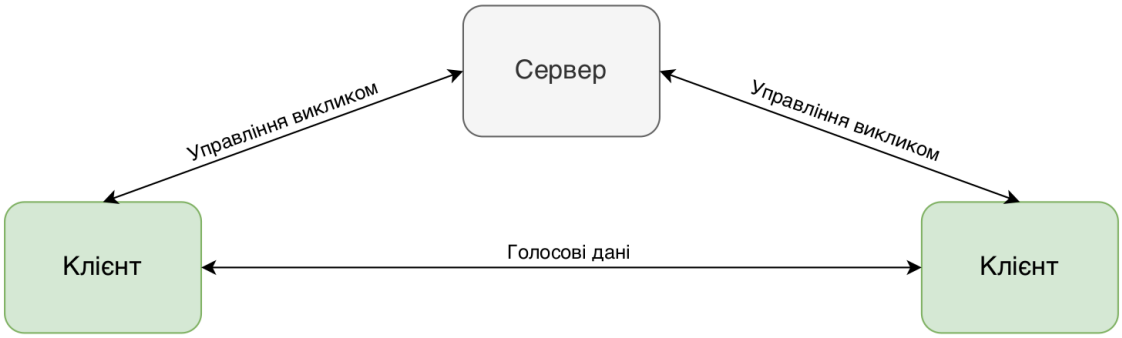

Рис. 1.7. Топологія гібридної мережі

Проблему реєстрації VoIP-клієнтів вирішує гібридна топологія на 1.7., що використовує сервер, але не для обміну голосовим трафіком, а для реєстрації та пошуку абонентів. Тим самим, сервер в даному випадку є як би АТС для цих двох абонентів. Саме гібридна топологія є найперспективнішою, оскільки вона не вимагає потужного сервера і каналу його зв'язку з Інтернет, але при цьому зберігає можливість централізованої реєстрації та пошуку абонентів.

Все це вірно, якщо говорити про VoIP-абонентів в Інтернет. Але ж VoIP-абоненти можуть спілкуватися не тільки між собою, але і дзвонити абонентам звичайної телефонної мережі і навіть отримувати від них дзвінки. Для вирішення цього завдання використовуються т.зв. VoIP-шлюзи, рис. 1.8. Це спеціальні пристрої, які здатні підключатися до мережі традиційної телефонії, але при цьому бути і абонентами VoIP-мережі. У підсумку виходить пристрій, який є як для VoIP-абонентів, так і для абонентів традиційної телефонії. Це дозволяє абонентам VoIP і традиційній телефонії дзвонити один одному через подібні шлюзи.

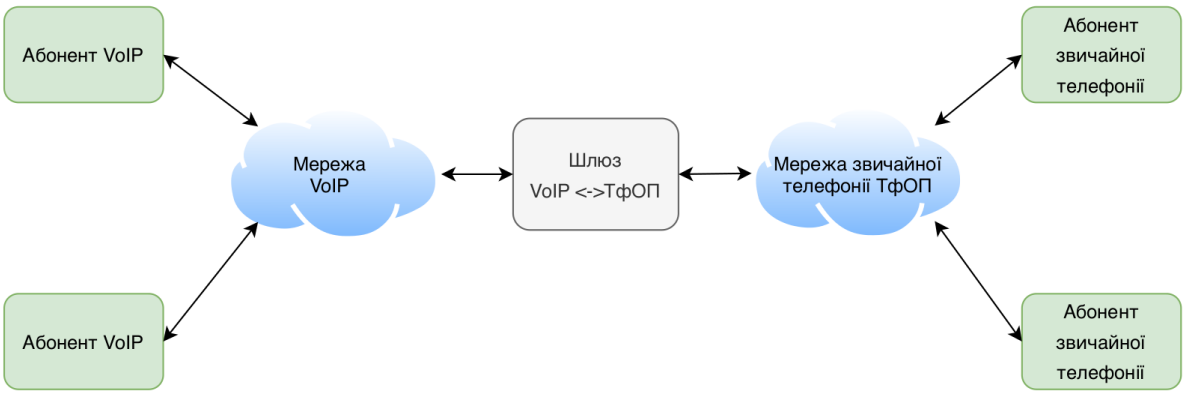

Рис. 1.8. Мережа звикористанням VoIP-шлюзу

Здавалося б, при використанні VoIP виникає стільки проблем, чи варто взагалі її використовувати? Відповідь на це питання далеко не завжди однозначна. Впершу чергу тому, що по кожному випадку варто реально оцінювати необхідність використання VoIP, а не звичайної телефонії.

Справа в тому, що VoIP може замінити традиційну телефонію, наприклад, на рівні підприємства. Якщо вирішити всі технічні проблеми VoIP, описані раніше, то ця технологія цілком може стати альтернативою офісним міні-АТС, оскільки має ряд переваг:

- не вимагає окремої проводки для телефонів - використовує існуючу мережу Ethernet;
- не вимагає власне міні-АТС, як пристрою, - досить запустити спеціальний сервіс на одному з наявних серверів;
- дозволяє вводити шифрування розмов на рівні телефонного апарату;
- легко інтегрується як з мережами VoIP, так і з мережами традиційної телефонії.

1.3. Рівні архітектури IP-телефонії

Архітектура технології Voice over IP може бути спрощена до двох площин. Нижня площина - це базова мережа з маршрутизацією IP-пакетів; верхня площина - це відкрита архітектура для управління обслуговуванням дзвінків (запитів зв'язку).

Нижня площина, простіше кажучи, - це комбінація відомих Інтернет-протоколів: це RTP (протокол транспорту в реальному часі), який діє поверх протоколу UDP (User Datagram Protocol), котрий, в свою чергу, розташований у стеку протоколів TCP / IP над протоколом IP. Таким чином, ієрархія RTP / UDP / IP є своєрідним транспортним механізмом для голосового трафіку. Тут ми також зазначимо, що в мережах з маршрутизацією IP-пакетів для передачі даних завжди передбачені механізми ретрансляції пакетів у разі втрати.

При передачі інформації в режимі реального часу використання таких механізмів лише погіршить ситуацію, тому для передачі інформації, яка чутлива до затримок, але менш чутлива до втрат, таких як дзвінки та відеоінформація, використовується механізм не гарантованої доставки інформації RTP / UDP / IP. Рекомендації ITU-T дозволяють затримки в одному напрямку не більше 150 мс. Якщо станція прийому вимагає повторної передачі пакета IP, затримки будуть занадто великими [1].

Тепер перейдемо до верхньої площини - управління обслуговуванням запитів зв'язку. Взагалі кажучи, управління послугами дзвінків передбачає вирішення, куди слід направляти виклик та як встановлювати зв’язок між абонентами. Інструментом такого управління є системи телефонної сигналізації, починаючи від систем, що забезпечують поєднання функцій маршрутизації та функцій створення комутаційного каналу розмови. В подальшому принципи сигналізації перетворилися на системи сигналізації за допомогою виділених сигнальних каналів, на багаточастотну сигналізацію, на протоколи сигналізації в масштабах загального каналу та на передачу функцій маршрутизації у відповідні вузли обробки служб інтелектуальної мережі.

У мережах з комутацією пакетів ситуація складніша. Мережа з маршрутизацією пакетів IP принципово підтримує одночасно ряд різних протоколів маршрутизації [2].

Це протоколи: RIP(Routing Information Protocol) - протокол маршрутної інформації, IGRP(Interior Gateway Routing Protocol) - протокол маршрутизації внутрішнього шлюзу, EIGRP(Enhanced Interior Gateway Routing Protocol) - розширений протокол маршрутизації внутрішнього шлюзу, IS-IS(Intermediate System-to-intermediate System) - протокол маршрутизації проміжних систем, OSPF(Open Shortest Path First) - протокол динамічної маршрутизації для знаходження найкоротшого шляху, BGP(Border Gateway Protocol) - протокол граничного шлюзу та інші. Таким же чином було розроблено низку протоколів для IP-телефонії.

Найбільш поширеним є протокол, специфікований в рекомендаціях H.323 ITU-T, зокрема, тому, що він став застосовуватися раніше інших протоколів, яких, до того ж, до впровадження H.323 взагалі не існувало.

Інший протокол площини управління обслуговуванням дзвінків – SIP (Session Initiation Protocol) - спрямований на те, щоб зробити термінальні пристрої та шлюзи більш розумними та підтримати додаткові послуги для користувачів.

Ще один протокол - SGCP - розроблявся щоб знизити вартість шлюзів шляхом впровадження функцій інтелектуальної обробки дзвінків у централізованому обладнанні. IPDC (Internet Protocol Device Control) дуже схожий на SGCP, але має набагато більше механізмів оперативного управління (OAM & P), ніж SGCP. Наприкінці 1998 року робоча група MEGACO комітету IETF розробила протокол MGCP, заснований в основному на протоколі SGCP, але з деякими доповненнями до частини OAM & P.

Робоча група MEGACO не зупинилася на досягнутому, продовжувала вдосконалювати протокол управління шлюзами і розробила більш функціональний, ніж MGCP, протокол MEGACO[1].

1.4. Протокол передачі даних SIP і його переваги над H.323

Протокол ініціації сесії (SIP) - це протокол на рівні додатків і призначений для організації, зміни та припинення сеансів зв'язку (мультимедійні конференції, телефонні з'єднання та розповсюдження мультимедійної інформації), які базуються на таких принципах:

• особиста мобільність користувачів. Користувачі можуть пересуватися без обмежень всередині мережі, тому послуги зв’язку повинні надаватися їм у будь-якій точці цієї мережі. Користувачу присвоюється унікальний ідентифікатор, а мережа надає йому послуги зв’язку незалежно від того, де він знаходиться. Для цього користувач, використовуючи спеціальне повідомлення - REGISTER - повідомляє сервер локації про свої рухи;

• визначення готовності користувача до участі в сеансі спілкування, для якого були введені спеціальні коди відповідей про поточну готовність користувача до спілкування;

• масштабованість мережі характеризується, перш за все, можливістю збільшення кількості мережевих елементів під час її розширення. Серверна структура мережі, побудована на основі протоколу SIP, повністю відповідає цій вимозі;

• розширюваність протоколу характеризується можливістю доповнення протоколу новими функціями при впровадженні нових сервісів та адаптації його до роботи з різними програмами;

• інтеграція в стек існуючих Інтернет-протоколів. SIP - частина глобальної мультимедійної архітектури, розроблена IETF (Internet Engineering Task Force);

• взаємодія з іншими сигнальними протоколами. SIP може використовуватися разом із протоколом H.323. Можлива також взаємодія протоколу SIP із сигналізаційними системами STOP - DSS1 та OKS7.

Однією з найважливіших особливостей протоколу SIP є його незалежність від транспортних технологій. Протоколи X.25, Frame Relay, AAL5, IPX тощо можуть використовуватися як транспорт. Структура повідомлень SIP не залежить від обраної технології транспорту. Але в той же час перевага віддається технології маршрутизації IP-пакетів та UDP.

Слід зазначити, що повідомлення сигналізації можуть переноситися не тільки протоколом транспортного рівня UDP, але і протоколом TCP. По мережі з маршрутизацією IP-пакетів може передаватися інформація користувача практично будь-якого виду: мова, відео та дані, а також будь-яка їх комбінація, що називається мультимедійною інформацією. Організовуючи зв’язок між терміналами користувача, необхідно повідомити протилежну сторону, яку інформацію можна отримувати (передавати), її алгоритм кодування та адресу, на котру вона повинна передаватися. Таким чином, однією з передумов організації зв'язку за допомогою протоколу SIP є обмін між призначеними учасниками комунікаційними даними щодо їх функціональних можливостей. Для цього найчастіше використовується протокол опису сеансу SDP (Session Description Protocol). Під час сеансу зв'язку він може бути модифікований, тому можливо передавати SIP-повідомлення з новими описами сеансів за допомогою інструментів SDP.

Комітет IETF пропонує використовувати протокол RTP для передачі голосової інформації, але протокол SIP не виключає можливості використання інших протоколів для цих цілей.

Також специфікація SIP визначає чотири основні функціональні елементи. Залежно від конкретних вимог, їх можна використовувати як окремі компоненти або комбінувати на інтегрованій платформі:

- агент користувача UA (User Agent або SIP-клієнт) - це додаток до обладнання терміналу і включає два компоненти: клієнт-агент користувача (Client User Agent Client - UAC) та сервер агента користувача (User Agent Server - UAS), інакше відомий як клієнт та сервер. Клієнт UAC ініціює SIP-

запити, тобто виступає в ролі абонента. Сервер UAS приймає запити і відповідає на них, тобто діє як викликана сторона;

- проксі-сервер (проксі-сервер) приймає запити, обробляє їх і відправляє далі на наступний сервер, який може бути або іншим проксі-сервером, або останнім UAS. Таким чином, проксі-сервер отримує та надсилає запити як від клієнта, так і від сервера. Прийнявши запит від UAC, проксі-сервер діє від імені цього UAC. Існує два типи проксі-служб: зі збереженням станів (stateful) і без збереження станів (stateless). Сервер першого типу зберігає вхідний запит у пам'яті, що стало причиною генерації одного або декількох вихідних запитів. Сервер також запам'ятовує ці вихідні запити. Усі запити зберігаються в пам'яті сервера лише до кінця транзакції, тобто до отримання відповідей на запитання. Сервер без збереження просто ретранслює запити та відповіді, які він отримує. Він працює швидше, ніж сервер 1-го типу, оскільки ресурс процесора не витрачається на зберігання станів, внаслідок чого сервер такого типу може обслуговувати більшу кількість користувачів. Проксі-сервер може змінювати запити, які він передає далі. Простіше кажучи, користувач надсилає запит на встановлення з'єднання з проксі-сервером, а той сам дбає про те, щоб воно було встановлено. Проксі-сервер може множити запит і надсилати його в різних напрямках, щоб запит досяг декількох місць, сподіваючись, що бажаний користувач опиниться в одному з них:

- Сервери перенаправлення призначені для передачі на запит поточної IP-адреси терміналу викликаного користувача. Сервер перенаправлення (або переадресації) передає клієнту відповіді на запит адреса наступного сервера або клієнта, з яким клієнт зв'язується потім безпосередньо. Для реалізації своїх функцій сервер перенаправлення повинен взаємодіяти з сервером локації;

- Сервери визначення місця розташування користувачів (реєстратори або сервери локації) надають агентам можливість реєструвати своє місцезнаходження. Сервер локації - адресна база даних, до якої звертаються SIP-сервери, які використовують її послуги для отримання інформації про можливе розташування викликаного користувача. Прийнявши запит, SIP-

сервер зв'язується з сервером локації, щоб дізнатися адресу, де можна знайти користувача. У відповідь видається або список можливих адрес, або повідомлення про неможливість їх пошуку.

Користувач може переходити від однієї термінальної системи до іншої, тому потрібен певний метод визначення його місцезнаходження, рис. 1.9.

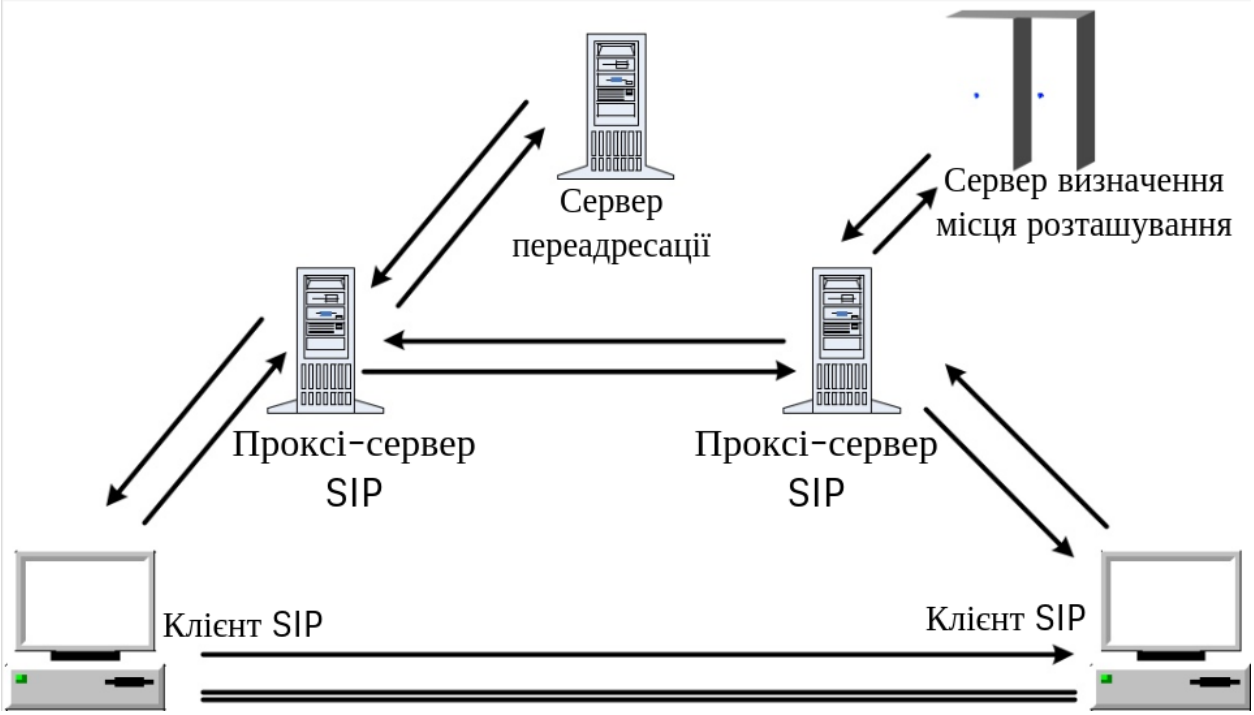

Рис. 1.9. Мережа IP-телефонії з сервером місця розтушування

Для цього SIP використовує сервер місця розташування - це база адрес, до яких звертаються SIP-сервери, які використовують його служби для отримання інформації про можливе місцезнаходження виклику користувача. Після прийняття запиту SIP-сервер зв'язується з сервером локації, щоб знайти адресу, де можна знайти користувача.

У відповідь він повідомляє або список можливих адрес, або інформує про неможливість їх пошуку. З іншого боку, користувач інформує SIP-сервер про своє місцезнаходження за допомогою повідомлення REGISTER. Сервер локації може розташовуватися як спільно з SIP-сервером, де можуть бути присутні деякі елементи бази адрес, так і окремо від нього.

А якщо говорити про порівняння SIP та H.323, то бидва протоколи вже досить давні - обидва вони створені наприкінці 90-х. H.323 працює на рівні бітових полів, що в ідеальних умовах реалізації (не в Інтернеті) дозволяє економити мережевий трафік порівняно з SIP. Однак у сучасних умовах швидкого поширення широкосмугового Інтернету ця перевага не виглядає настільки суттєвою. SIP - це протокол рівня додатків, що працює в мережевій моделі OSI.

Але якщо говорити про переваги SIP, то їх достатньо щоб зробити вибір в його користь:

- Простота: включає лише шість методів.
- Незалежність від транспортного рівня: може використовувати UDP, TCP, ATM тощо.
- Особиста мобільність користувачів. Користувачі можуть пересуватись в межах мережі без обмежень, призначаючи користувачеві унікальний ідентифікатор.
- Масштабованість мережі. Мережева структура на основі протоколу SIP дозволяє легко розширювати та збільшувати кількість елементів.
- Розширюваність протоколу. Протокол характеризується можливістю доповнювати його новими функціями при появі нових служб.
- Інтеграція в стек існуючих протоколів Інтернет. SIP є частиною глобальної мультимедійної архітектури, розробленої IETF. Ця архітектура також включає RSVP, RTP, RTSP, SDP.
- Взаємодія з іншими сигнальними протоколами. SIP може використовуватися разом з іншими протоколами IP-телефонії, протоколами PSTN та для зв'язку з розумними мережами.

Також немало важливим являється те, що SIP - це протокол, який є найбільш зрозумілим для людей, тому розробляти та підтримувати програмне забезпечення для SIP простіше, ніж H.323.

За рахунок більш простої реалізації, в порівнянні з H.323, SIP-зв'язок став популярною VoIP-послугою, що надається багатьма постачальниками послуг IP-телефонії, яка підключається до телефонної мережі загального користування (ТМЗК) через Інтернет. Тому можна вважати використання протоколу SIP більш перспективним.

1.5. Типи VoIP-пристроїв та можливі схеми їх підключення

З розвитком послуг IP-телефонії зростає і ринок VoIP обладнання. І для кожної компанії важливо, щоб обладнання було зручним у використанні і працювало стабільно.

Далі йде розповідь про те, які види кінцевого VoIP обладнання існують, переваги та недоліки кожного виду, і які більш стабільні для використання в мережах IP-телефонії.

1)Дротові IP-телефони з дротовим мережним підключенням.

Переваги:

- Найбільш надійне з усіх типів VoIP-обладнання
- Вони рідко виходять з ладу, проміжне обладнання не потрібно для підключення до SIP (окрім маршрутизатора), вони підключаються до мережі проводом, живленням від електрики. Завдяки цим фактором пристрої стабільно підтримують SIP реєстрацію, мають хорошу якість зв'язку та тривалий термін слугування
- Легко налаштувати
- Легко підключити
- Ідеально підходить для телефонного центру та технічної підтримки, оскільки є можливість підключити професійну гарнітуру
-

Недоліки:

- Мобільність
- Потрібен додатковий простір для обладнання

Ці пристрої можна підключити за двома схемами на рис. 1.10:

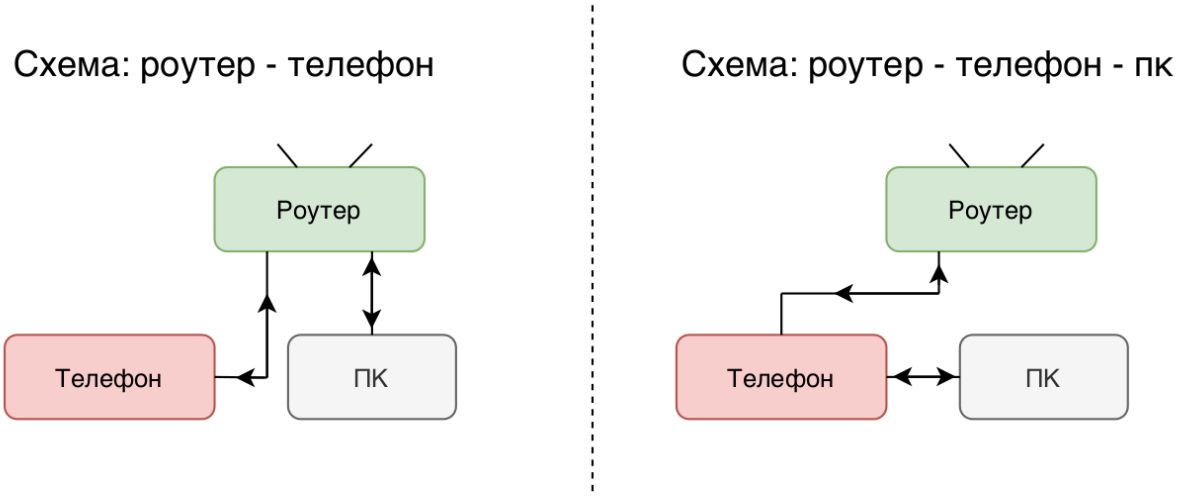

Рис. 1.10 Схеми підключення дротових пристроїв

2) IP-телефони з дротовою гарнітурою, що підключаються до мережі по Wi-Fi.

Взагалі то ситуація у даного виду обладнання практично така ж, що і у попереднього представника. Додається тільки ще по одній перевазі та недоліку.

Перевага:

- Зручні в підключенні. Немає необхідності тягнути дроти до кожного апарату, що скорочує рівень витрат на комутацію

Недолік:

- Якість зв'язку і стабільність підключення до SIP безпосередньо залежить від якості Wi-Fi сигналу. Виникає необхідність використовувати Wi-Fi репітери.

3) Бездротові IP-телефони, прив'язаною до основної бази, котра відповідно з'єднана дротом з мережею.

Переваги:

- Досить надійне обладнання
- Мобільні в використанні
- Економлять ресурси підключення. Проводом до мережі підключається тільки основна база
- До однієї бази можна підключити до 8 пристроїв

Недоліки:

- Погіршення якості зв'язку в залежності від відстані між трубкою і базою
- Потрібно додатковий елемент живлення
- Можливі погіршення стабільності роботи в разі великого навантаження на одну базу
- Досить складні в налаштуванні
- Є ймовірність від'єднання пристрою від бази

Схема підключення на рис. 1.11:

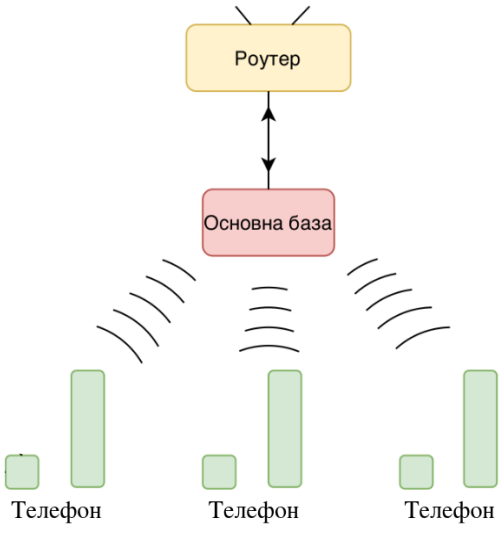

Рис. 1.11. Схема підключення бездротових пристроїв

4)Дротові аналогові телефони котрі підключаються через голосовий VoIP-шлюз.

Переваги:

- Можливість використання в ір-телефонії апаратів, що залишилися від старої аналогової телефонії
- Простота підключення до VoIP шлюзу
- Довговічність

Недоліки:

- Безпосередньо залежать від VoIP шлюзу і якості підключеного патч-корду
- Ймовірність перемикання в імпульсний режим
- Ймовірність проблем зі зв'язком аналогового характеру
- Налаштування VoIP шлюзу часто викликає труднощі навіть у системних адміністраторів
- Мають нестабільне підключення до SIP (іноді вимагають перезавантаження VoIP шлюзу)

3 можливі схеми підключення, рис. 1.12:

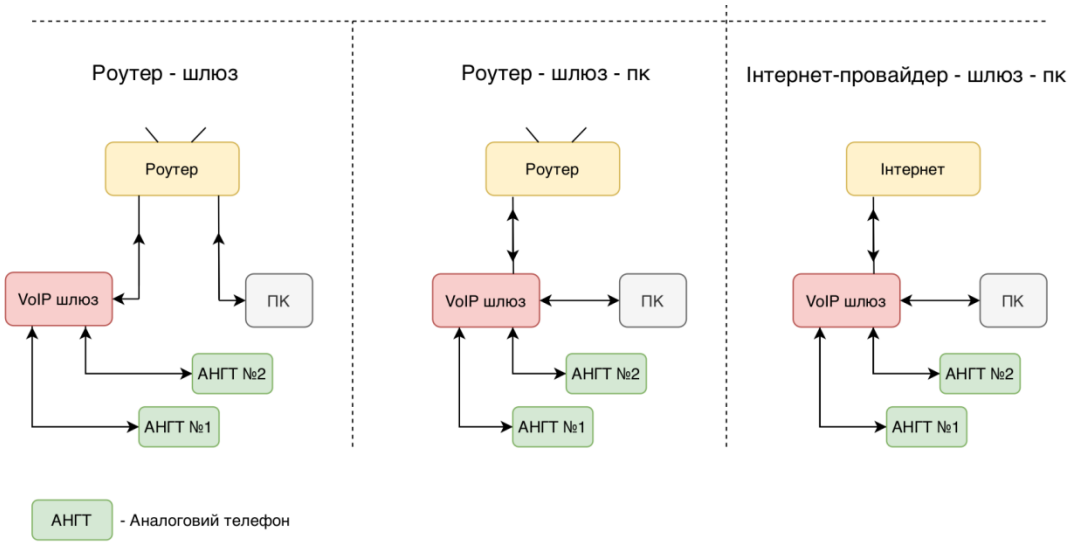

Рис. 1.12. Схема підключення пристроїв звикористанням VoIP-шлюзу

5)Бездротові аналогові телефони підключаються через голосовий VoIP-шлюз

Ситуація практично така ж, що і у попереднього виду аналогових апаратів. Додається кілька переваг і недоліків.

Переваги:

- Мобільність
- Не займають додаткового простору при встановленні

Недоліки:

- Можливо погіршення якості зв'язку в залежності від відстані до бази, або наявність перешкод радіоканалу
- Необхідний додатковий елемент живлення

6)Програмні ip-телефони (софтфони) для дзвінків з ПК і ноутбуків.

Софтфон - це програма, яка імітує телефон на вашому комп'ютері і дозволяє дзвонити і приймати дзвінки через IP-телефонію (VoIP). Для того, щоб дзвонити через софтфон, потрібна гарнітура або мікрофон + динаміки.

Перевага софтфона перед апаратним IP-телефоном - багатий інтерфейс, не обмежений маленьким телефонним екраном. Тому Софтфони можуть надавати додаткові можливості, наприклад, телефонну книгу, індикацію онлайн-статусу, відеодзвінки, передачу текстових повідомлень, факсів. По суті, софтфон - це те ж саме, що просунутий месенджер.

Існують софтфони, які працюють тільки з певним VoIP-провайдером і універсальні софтфони, які можуть використовуватися з різними провайдерами, які підтримують найпоширеніший протокол SIP.

Переваги:

- Безкоштовні
- Не вимагають додаткової комутації мережі для підключення
- Встановлюються на будь-який ПК і ОС
- Легко налаштовуються

Недоліки:

- Безпосередньо залежать від швидкодії та працездатності ПК
- Досить нестабільні в роботі (потрібно перезапуск програми, або всього ПК)
- Для гарної якості зв'язку потрібно дротове підключення ПК до роутера

Незважаючи на мінуси, даний вид VoIP пристроїв завоював велику популярність у використанні.

1.6. Оцінка надійності та фактори які впливають на стабільність роботи IP-пристроїв.

Таблиця 1.1

Оцінка надійнсотіпристроїв

Оцінка надійності	Тип IP-пристрою	Спосіб підключення	Фактори які впливають на стабільність
10	Дротовий IP-телефон	Провід(вита пара)	1)патч-корд від пристрою до світч або роутера 2)локальна мережа або маршрутизуючі пристрої 3)мережа Інтернет провайдера 4)сам пристрій
9	Бездротовий IP-телефон з базою	Провід(вита пара)	1)дальність прийому сигналу між базою і пристроєм 2)радіоперешкоди 3)патч-корд від пристрою до світч або роутера 4)локальна мережа або маршрутизуючі пристрої 5)мережа Інтернет провайдера 6)сам пристрій
8	Дротовий IP-телефон(Wi-Fi)	Wi-Fi	1)дальність прийому сигналу між роутером і пристроєм 2)радіоперешкоди Wi-Fi сигналу 3)локальна мережа або маршрутизуючі пристрої 4)мережа Інтернет провайдера

Продовження таблиці 1.1 Оцінка надійності пристроїв

7	Аналоговий телефон і VoIP шлюз	Провід(вита пара)	1)патч-корд від VoIP шлюза до світч або роутера 2)патч-корд від VoIP шлюза до пристрою 3)локальна мережа або маршрутизуючі пристрої 4)мережа Інтернет провайдера 5)сам пристрій 6)сам VoIP шлюз
6	Софтфон на ПК	Провід(вита пара)	1)патч-корд від ПК до світч або роутера 2)локальна мережа або маршрутизуючі пристрої 3)мережа Інтернет провайдера 4)сам ПК 5)сам Софтфон 6)гарнітура
5	Софтфон на ноутбуці	Wi-Fi	1)дальність прийому сигналу між роутером і ноутбуком 2)радіоперешкоди Wi-Fi сигналу 3)локальна мережа або маршрутизуючі пристрої 4)мережа Інтернет провайдера 5)сам Ноутбук 6)сам Софтфон 7)гарнітура

Висновки:

В цьому розділі було розглянуто загальну інформацію про мережу IP-телефонії, тобто: те як працює мережа ip-телефонії; архітектуру та топологію мережі. Було розглянуто протоколи передачі даних SIP та H.323, виявлено що на даний момент доцільніше використовувати протокол SIP при побудові мережі. Проведено порівняння різних кінцевих пристроїв пристроїв, які використовуються в мережах IP-телефонії та показані можливі схеми їх підключення. Було представлено їх недоліки та переваги, та їх кінцеве порівняння то критерію безпеки та надійності.

РОЗДІЛ 2

ЗАГРОЗИ ТА МЕТОДИ ЗАХИСТУ В МЕРЕЖАХ IP-ТЕЛЕФОНІЇ

2. Види загроз в IP-телефонії та методи боротьби з ними

Конфіденційність та безпека є обов'язковими вимогами до будь-якої телефонної мережі. З часом вдалося забезпечити певний, хоча і далеко не ідеальний, рівень безпеки в традиційних мережах. Поширення IP-телефонії та її претензія стати головною технологією передачі голосу в найближчому майбутньому викликають ряд проблем, з якими традиційна телефонія ніколи не стикалася, або давно забула, або вже навчилася справлятися.

У корпоративних колах сьогодні є як опоненти, так і прихильники впровадження IP-телефонії як альтернативної технології передачі голосу. І якщо перші, як то кажуть, не повинні турбуватися, то останні повинні знати, що нові конвергентні мережі та голосові послуги також вводять нові вразливості для мереж [3].

2.1. Види загроз в IP телефонії

Питання безпеки зв'язку завжди був одним з важливих в мережах телекомунікацій. В даний час у зв'язку з бурхливим розвитком глобальних комп'ютерних мереж, і в тому числі мереж Інтернет-телефонії, забезпечення безпеки передачі інформації стає ще більш актуальним. Розробка заходів в області безпеки повинна проводитися на основі аналізу ризиків, визначення критично важливих ресурсів системи і можливих загроз. Існує кілька основних типів загроз, які становлять найбільшу небезпеку в мережах IP-телефонії [3]:

- **Підміна даних** про користувача означає, що один користувач мережі видає себе за іншого. При цьому виникає вірогідність

несанкціонованого доступу до важливих функцій системи. Використання механізмів автентифікації і авторизації в мережі підвищує впевненість в тому, що користувач, з яким встановлюється зв'язок, не є підставною особою і що йому можна надати санкціонований доступ [3].

- **Прослуховування**. Під час передачі даних про користувачів (призначених для користувача ідентифікаторів і паролів) або приватних конфіденційних даних по незахищених каналах ці дані можна підслухати і згодом зловживати ними. Методи шифрування даних знижують ймовірність цієї загрози [3].

- **Маніпулювання даними**. Дані, які передаються по каналах зв'язку, в принципі можна змінити. У багатьох методах шифрування використовується технологія захисту цілісності даних, що запобігає їх несанкціонованих змін [3].

- **Відмова від обслуговування** (Denial of Service - DoS) є різновидом хакерської атаки, в результаті якої важливі системи стають недоступними. Це досягається шляхом переповнення системи непотрібним трафіком, на обробку якого йдуть всі ресурси системної пам'яті і процесора. Система зв'язку повинна мати кошти для розпізнавання подібних атак і обмеження їх впливу на мережу [3].

- Найбільш розвиненою формою шахрайства в Інтернет, без сумніву, є **фішинг**. Типовими інструментами фішингу є mail (поштові повідомлення, що використовують методи соціальної інженерії), спеціально розроблені web-сайти.

Представляючи новий звіт, учасники антифішингової робочої групи (APWG) відзначили, що в 2 кварталі активність фішерів продовжувала

зростати. За три місяці активісти занесли в базу інформацію про 182 465 підроблених сайтах - проти 180 768 в попередньому кварталі. Число фішингових атак (унікальних email-розсилок) залишилося на колишньому рівні - трохи більше 112 тисяч [4].

Статистика за 2 квартал 2019 року, табл. 2.1:

Таблиця 2.1

Статистика фішинг-сайтів

	Квітень	Жовтень	Листопад
Кількість виявлених веб-сайтів, що фішингують	59,756	61,820	60,889
Кількість унікальних фішинг-звітів (кампаній) переданих в APWG	37,054	40,177	34,932
Кількість брендів, націлених на фішинг-кампанії	341	308	289

Загальна кількість фішинг-сайтів, виявлених APWG в 2 кварталі, склала 182 465, що трохи більше порівняно з 180 768 зафіксовано у 1 кварталі 2019 р. та, особливо відрізняється від 138288, що спостерігалися у 4 кварталі 2018 року та 151,014 у 3 кварталі 2018 році, рис. 2.1 [4].

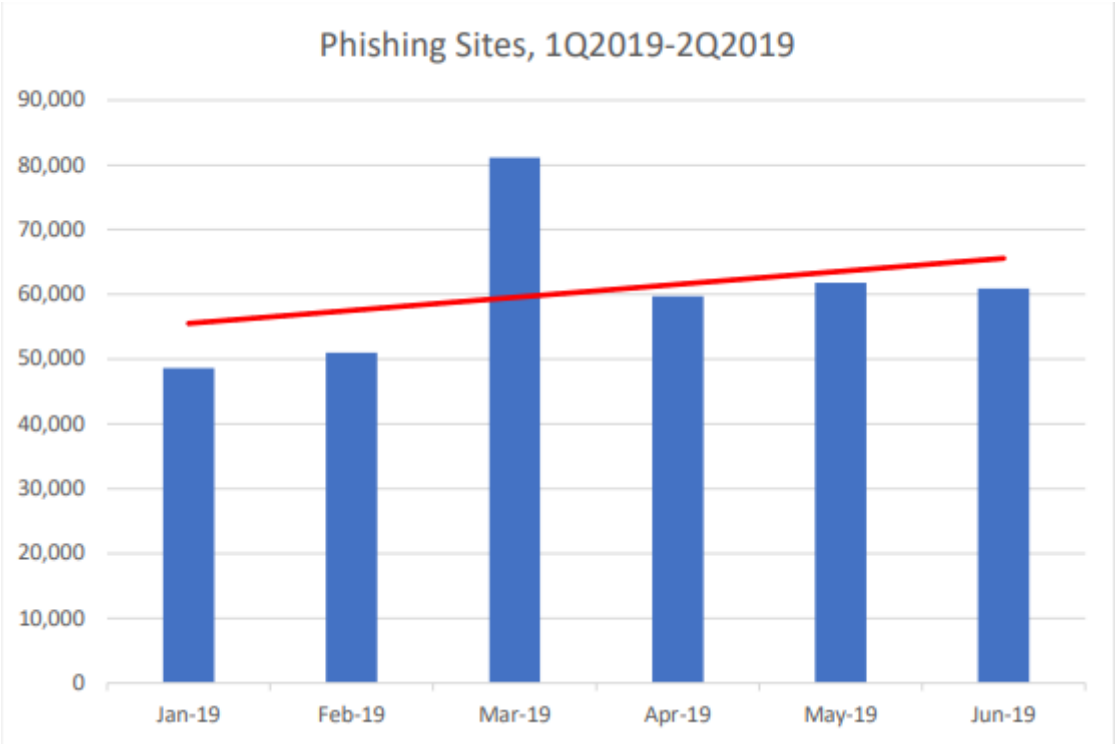

Рис. 2.1 Діаграма кількості фішинг-сайтів протягом 2019 року

Базовими елементами в області безпеки є автентифікація, цілісність і активна перевірка. Автентифікація покликана запобігти загрозі знеособлення і несанкціонованого доступу до ресурсів і даних. Хоча авторизація не завжди включає до свого складу автентифікацію, але частіше за все одне обов'язково має на увазі інше. Цілісність забезпечує захист від прослуховування і маніпулювання даними, підтримуючи конфіденційність і незмінність переданої інформації. І, нарешті, активна перевірка означає перевірку правильності реалізації елементів технології безпеки і допомагає виявляти несанкціоноване проникнення в мережу і атаки типу DoS.

2.2. Методи криптографічного захисту інформації

Основою будь-якого безпечного з'єднання є криптографія. Криптографія - це технологія складання та розшифрування зашифрованих повідомлень. Крім того, криптографія є важливим компонентом механізмів автентифікації,

цілісності та конфіденційності. Автентифікація - це засіб перевірки особи відправника або одержувача інформації. Цілісність означає, що дані не були змінені, а конфіденційність створює ситуацію, коли ніхто, крім відправника та одержувача, не може зрозуміти дані. Зазвичай криптографічні механізми існують у вигляді алгоритму (математична функція) та секретного значення(ключа). Алгоритми широко відомі, тільки криптографічні ключі потрібно зберігати в секреті. І чим більше бітів у цьому ключі, тим він менш вразливий

Системи безпеки використовують три основні криптографічні методи:

- симетричне шифрування;
- асиметричне шифрування;
- односторонні хеш-функції.

Всі існуючі технології автентифікації, цілісності та конфіденційності створюються на основі цих трьох методів. Наприклад, цифрові підписи можуть бути представлені у вигляді комбінації асиметричного шифрування з алгоритмом односторонньої хеш-функції для підтримки автентифікації та цілісності даних.

Симетричне шифрування, яке часто називають шифрованим секретним ключем, в основному використовується для забезпечення конфіденційності даних. У цьому випадку двоє користувачів повинні спільно вибрати єдиний математичний алгоритм, який буде використовуватися для шифрування та дешифрування даних. Крім того, їм потрібно вибрати загальний ключ (секретний ключ), який буде використовуватися з прийнятим ними алгоритмом шифрування / дешифрування.

В даний час широко використовуються таємні ключові алгоритми, такі як стандарт шифрування даних DES (Data Encryption Standard), 3DES (або "потрійний DES") та міжнародний алгоритм шифрування даних IDEA (International Data Encryption Algorithm). Ці алгоритми шифрують повідомлення блоками з 64 біт. Якщо повідомлення перевищує 64 біт (як це

зазвичай буває), необхідно розбити його на блоки по 64 біти кожен, а потім якось з’єднати їх. Таке поєднання, як правило, відбувається одним із наступних чотирьох методів: електронною кодовою книгою ECB (Electronic codebook), ланцюжком зашифрованих блоків CBC (Cipher block chaining), x-бітним зашифрованим зворотним зв'язком CFB-x (Cipher feedback) або вихідним зворотним зв'язком OFB (Output feedback).

Шифрування секретним ключем найчастіше використовується для підтримки конфіденційності даних і дуже ефективно реалізується за допомогою незмінних «дротових» програм (прошивок). Цей метод можна використовувати для автентифікації та підтримки цілісності даних, але метод цифрового підпису є більш ефективним.

Метод секрктного ключа має такі недоліки:

- часто потрібно змінювати секретні ключі, оскільки завжди існує ризик їх випадкового розкриття;
- важко безпечно генерувати та поширювати приватні ключі.

Асиметричним шифруванням часто називають загальне шифрування ключів, яке використовує різні, але взаємодоповнюючі ключі та алгоритми шифрування та розшифрування. Цей механізм спирається на два взаємопов’язані ключі: відкритий ключ та приватний ключ. Найпоширеніші приклади використання алгоритмів спільних ключів:

- конфіденційність даних;
- автентифікація відправника
- надійно отримати загальні ключі для спільного використання.

Важливим аспектом асиметричного шифрування є те, що приватний ключ повинен залишатися приватним. Якщо приватний ключ розкрито, то особа, яка знає цей ключ, зможе говорити від імені клієнта, отримувати

повідомлення від цього клієнта та надсилати повідомлення так, як ніби це робив клієнт.

Механізми генерації пар відкритих / приватних ключів досить складні, але в результаті виходить пара дуже великих випадкових чисел, одне з яких стає відкритим, а інше приватним ключем. Генерація таких чисел вимагає великих процесорних потужностей, оскільки ці числа, як і їх продукція, повинні відповідати суворим математичним критеріям. Однак цей процес генерації абсолютно необхідний для забезпечення унікальності кожної пари відкритих / приватних ключів. Алгоритми шифрування загальних ключів рідко використовуються для підтримки конфіденційності даних через обмеження продуктивності. Натомість вони часто використовуються в додатках, де автентифікація здійснюється цифровим підписом та керуванням ключами.

Серед найбільш відомих загальних ключових алгоритмів - RSA та ElGamal.

Безпечна хеш-функція - це функція, яку легко обчислити, але зворотне відновлення вимагає набагато більшого обсягу зусиль. Вхідне повідомлення передається через математичну функцію (хеш-функція), і в результаті на виході отримується певна послідовність бітів. Ця послідовність називається "хеш" (або "результат обробки повідомлень"). Цей процес неможливо відновити.

Хеш-функція приймає повідомлення будь-якої довжини і видає хеш фіксованої довжини на виході.

Загальні хеш-функції включають:

- алгоритм Message Digest 4 (MD4)
- алгоритм Message Digest 5 (MD5)
- алгоритм безпечного хешу SHA (Secure Hash Algorithm)

Технологія шифрування часто використовується в програмах управління ключами та автентифікації. Наприклад, алгоритм Діффі-Гелмана дозволяє двом сторонам створити спільну для них таємницю, відому лише

обом обом, незважаючи на те, що зв'язок між ними здійснюється через незахищений канал. Потім цей приватний ключ використовується для шифрування даних за допомогою алгоритму приватного ключа. Важливо зазначити, що поки що не створено засобів для визначення автора такого ключа, тому обмін повідомленнями, зашифрованими таким чином, може бути предметом хакерських атак. Алгоритм Діффі-Хеллмана використовується для підтримки конфіденційності даних, але не використовується для автентифікації. Автентифікація в цьому випадку досягається за допомогою цифрового підпису.

Цифровий підпис - це зашифрований хеш, який додається до документа. Він може використовуватися для автентифікації відправника та цілісності документа. Цифрові підписи можна створити за допомогою комбінації хеш-функцій та криптографії відкритого ключа.

Повідомлення, яке надсилається по каналу зв'язку, складається з документа та цифрового підпису. На іншому кінці каналу зв'язку повідомлення поділяється на оригінальний документ та цифровий підпис. Оскільки цифровий підпис був зашифрований приватним ключем, його можна розшифрувати в кінці прийому за допомогою спільного ключа. Таким чином, на кінці отримання виходить розшифрований хеш. Далі текст документа вводиться на вхід тієї самої функції, яку використовувала передавальна сторона. Якщо вихід має той самий хеш, який був отриманий у повідомленні, цілісність документа та особи відправника можна вважати вірними.

Цифровий сертифікат - це цифрово підписане повідомлення, яке в даний час зазвичай використовується для перевірки спільного ключа. Цифровий сертифікат у стандартному форматі X.509 включає такі елементи:

- номер версії;
- серійний номер сертифіката;
- емітент інформації про алгоритм;
- емітент сертифікату;
- дати початку і закінчення дії сертифіката;

- інформація про алгоритм загального ключа суб'єкта сертифіката;

Загальний вигляд криптографічного системи можна представити в такий спосіб, рис. 2.2:

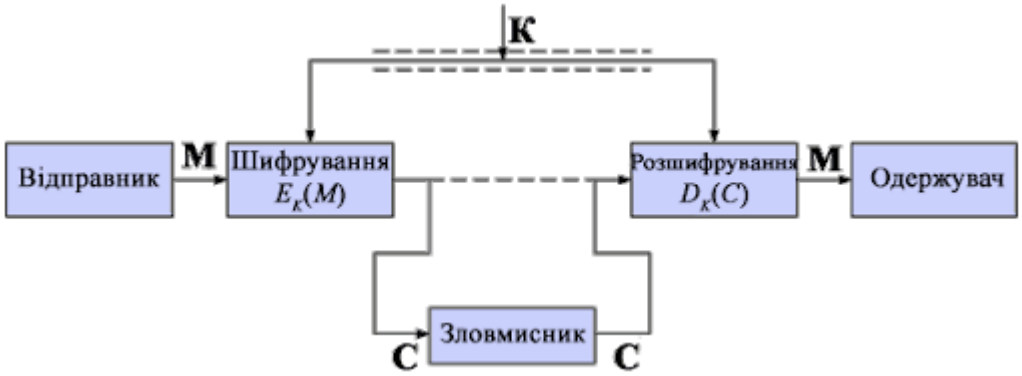

Рис. 2.2. Криптографічна система

Для використання такої системи для певного повідомлення M вибирається деякий ключ K з множини можливих ключів K. Після чого за допомогою ключа K формується криптограма. Ця криптограма, отримана за допомогою перетворення Ek(M), по каналу передачі передається в точку прийому. На приймальному кінці за допомогою відображення Dk(C), зворотного до заданої, з криптограми відновлюється вихідне повідомлення M.

Якщо зловмисник перехопить криптограму, то він не зможе її розшифрувати, якщо не знає ключа K. Тому, чим більше потужність множини K, тим менше ймовірність того, що криптограма буде розшифрована. Ця ймовірність називається апостеріорної ймовірністю. Обчислення апостеріорного ймовірностей - є спільне завдання дешифрування.

Рис. 2.3. Види криптографічних алгоритмів

За характером використання ключа всі криптосистеми можна поділити на симетричні (одноключеві із секретним ключем) та асиметричні (асиметричні, із відкритим ключем), рис. 2.3. У першому випадку той самий ключ використовується як для шифрування, так і для дешифрування. Це таємно і передається відправником одержувачу через канал зв'язку, який виключає перехоплення. В асиметричних системах для шифрування та розшифровки використовуються різні ключі, пов'язані між собою якоюсь математичною залежністю. Більше того, залежність така, що дуже важко обчислити інший ключ з одного ключа протягом прийнятного періоду часу.

Функції шифрування та дешифрування, залежно від алгоритму, можуть бути однаковими або, найчастіше, різними, а процес дешифрування є зворотнім процесом шифрування.

Вся різноманітність симетричних криптографічних систем базується на таких класах:

- **Блочні шифри**. Вони являють собою сімейство зворотних перетворень блоків (частин фіксованої довжини) вихідного тексту. Фактично блок-шифр - це система заміщення блоків. Після розбиття тексту на блоки, кожен блок шифрується окремо, незалежно від його положення та послідовності введення.

Один з найпоширеніших способів визначення блокових шифрів - це використання так званих мереж Feistel. Мережа Feistel - це загальний метод перетворення довільної функції в перестановку на багатьох блоках.

- **Шифр заміни**. Замінні (підстановочні) шифри - це найпростіший вид перетворень, який полягає в заміні символів вихідного тексту іншими (того ж алфавіту), за більш-менш складним правилом. Заміни розрізняють одно алфавітні та багатоалфавітні. У першому випадку кожен символ вихідного тексту перетворюється в символ шифротексту відповідно до того ж закону. При багатоалфавітній підстановці закон змінюється від символу до символу. Цей клас включає так звану одноразову систему ключів.
- **Перестановочні шифри**. Перестановки - метод криптографічного перетворення, який полягає в обміні символами вихідного тексту за деяким правилом. Перестановочні шифри наразі не використовуються в чистому вигляді, оскільки їх криптографічна сила недостатня.
- **Шифр XOR** - це перетворення, при якому символам вихідного тексту додається модуль, рівний потужності алфавіту, причому символи псевдовипадкової послідовності породжуються певним правилом. В принципі, шифр XOR не можна виділити в окремий клас криптографічних перетворень, оскільки ця псевдовипадкова послідовність може бути сформована, наприклад, за допомогою блокового шифру.
- **Потокові шифри**. Потокові шифри - це різновид шифру XOR і він перетворює звичайний текст в зашифрований один за одним. Генератор послідовностей ключів створює послідовність бітів K1, K2, ..., Ki, ... Ця послідовність ключів сумується по модулю 2 до послідовності бітів вихідного тексту P1, P2, ..., Pi,. .. для отримання шифротексту Ci = Pi * Ki. На приймальній стороні текст складається по модулю 2 з однаковою послідовністю ключів для отримання вихідного тексту. Однак для шифрування потоку для збільшення криптографічної сили генератор ключових послідовностей "прив'язується" до поточного стану кодованого

символу. Тобто значення, що генеруються, залежать не тільки від ключа, але і від кількості зашифрованого біта та послідовності введення.

2.3. Захист від прослуховування

Що стосується прослуховування звичайної телефонної лінії, існує декілька загальних методів підключення до мережі. Перший і найпростіший спосіб - підключити паралельний телефон до тієї ж лінії. Цей метод працює не тільки для дротових телефонів, але і для бездротових телефонів. У цьому випадку потрібно змусити обидва телефони працювати з однаковою частотою.

Найпопулярніший метод прослуховування телефонів - підключити так званий “жучок” до комутатора, який обробляє ваші дзвінки. Оскільки отримати доступ до комутатора просто неможливо, такий спосіб прослуховування залишається прерогативою спеціальних служб. Вони також можуть підключатися до центральних магістралей і одночасно записувати мільйони дзвінків. Ці методи працюватимуть і для мобільних пристроїв.

Зловмисники найчастіше використовують уразливості сучасних смартфонів для прослуховування. Зламавши телефон, вони можуть встановити програму прослуховування або відстеження. Такий додаток створить програмний шлюз, який буде перенаправляти дзвінки на потрібний номер телефону і, таким чином, прослуховувати дзвінок.

Донедавна IP-телефонія була єдиним непроникним засобом зв'язку. На початок зазначимо, що протокол VoIP передбачає передачу голосових повідомлень, які поділяються на пакети через Інтернет на основі протоколу TCP / IP. В принципі голосовий зв’язок через IP порівнянний із завантаженням файлу з локального комп'ютера на віддалений сервер. У цьому випадку кожен, хто має доступ до вашого ПК або до будь-якого пристрою, через який проходить ваш трафік, може перехопити ваші голосові пакети. Хитрість полягає в тому, що, захопивши пакети, зловмисник взагалі нічого не отримає,

тому що всі пакети шифруються, коли їх надсилають. У вашого співрозмовника є той самий ключ, який дозволяє його ПК розшифрувати пакет і перетворити повідомлення назад у голосове повідомлення.

Також для захисту VoIP-телефонії від прослуховування на місцевому рівні може бути підключена окрема закрита локальна мережа, до якої можна підключити будь-який IP-телефон. Однак, як ми вже говорили, це рішення підходить для невеликого офісу; дзвінки на великі відстані не можуть бути захищені цим методом.

Однак головна небезпека полягає в очікуванні користувачів на їхніх локальних машинах. Насправді в більшості випадків перехоплення пакетів відбувається, коли вони доходять до абонента і розшифровуються. Перехоплення дзвінка таким чином набагато простіше, ніж злом шифрування пакетів, тому захист VoIP-комунікацій перетворюється, по суті, на захист вашого ПК та локальної мережі від злому.

2.4. Технології автентифікації

Використання відкритих каналів передачі даних створює потенційні можливості для дій зловмисників. Тому одним із важливих завдань забезпечення інформаційної безпеки під час взаємодії з користувачем є використання методів та засобів, що дозволяють одній стороні (що верифікує) перевірити справжність іншої (перевіряється) сторони. Зазвичай для вирішення цієї проблеми застосовуються спеціальні прийоми, які дають можливість перевірити справжність перевіреної сторони.

Кожен суб'єкт, зареєстрований у комп'ютерній системі (користувач або процес, що діє від імені користувача), пов'язаний з деякою інформацією, яка однозначно його ідентифікує. Це може бути число або рядок символів, що іменують даний суб'єкт. Ця інформація називається ідентифікатором суб'єкта. Якщо у користувача є ідентифікатор, зареєстрований у мережі, він вважається

законним користувачем; інші - нелегальні користувачі. Перш ніж отримати доступ до ресурсів комп'ютерної системи, користувач повинен пройти процес первинної взаємодії з комп'ютерною системою, що включає автентифікацію.

Автентифікація - процедура автентифікації для заявленого користувача, процесу чи пристрою. Ця перевірка дозволяє надійно переконатися, що користувач (процес чи пристрій) саме те, що він заявляє про себе. Проводячи автентифікацію, сторона яка перевіряє переконується у справжності перевіреної сторони, тоді як перевірена сторона також активно бере участь в обміні інформацією. Зазвичай користувач підтверджує свою особу, вводячи в систему унікальну інформацію, невідому іншим користувачам про себе (наприклад, пароль або сертифікат).

Процеси автентифікації також можна класифікувати за рівнем забезпеченості. Відповідно до цього **процеси автентифікації поділяються на такі типи:**

- автентифікація за допомогою паролів та PIN-кодів;
- сильна автентифікація, заснована на використанні криптографічних методів та інструментів;
- біометрична автентифікація користувача.

З точки зору безпеки, кожен із цих типів сприяє вирішенню конкретних завдань, тому процеси автентифікації та протоколи активно використовуються на практиці.

Основні атаки на протоколи автентифікації:

- користувач видає себе за іншого, щоб отримати повноваження та можливість діяти від імені іншого користувача;
- заміна сторони обміну автентифікацією (атака перемежування). Зловмисник під час цієї атаки бере участь в обміні автентифікацією між двома сторонами з метою зміни трафіку, що проходить через нього;
- повторна атака полягає у повторній передачі даних автентифікації будь-яким користувачем;

- вимушена затримка. Зловмисник перехоплює якусь інформацію і через деякий час передає її;

- атака з вибором тексту {атака вибраного тексту). Зловмисник перехоплює трафік автентифікації та намагається отримати інформацію про довгострокові криптографічні ключі.

Для запобігання таких атак при складанні протоколів автентифікації використовуються наступне:

- використання запиту-відповіді, часової позначки, випадкових чисел, ідентифікаторів, цифрових підписів;

- зв'язування результату автентифікації з подальшими діями користувачів всередині системи. Прикладом такого підходу є реалізація в процесі автентифікації обміну секретними сеансовими ключами, які використовуються під час подальшої взаємодії з користувачем;

- періодичні процедури автентифікації в рамках вже встановленого сеансу зв'язку тощо.

Механізм «запит-відповідь» полягає в наступному. Якщо користувач А хоче бути впевненим, що повідомлення, одержувані ним від користувача В, не є помилковими, він включає в посилається для В повідомлення непередбачуваний елемент - запит Х (наприклад, деякий випадкове число). При відповіді користувач В повинен виконати над цим елементом деяку операцію (наприклад, обчислити деяку функцію). Це неможливо здійснити заздалегідь, так як користувачу В невідомо, яке випадкове число Х прийде в запиті. Отримавши відповідь з результатом дій В, користувач Л може бути впевнений, що В - справжній. Недолік цього методу - можливість встановлення закономірності між запитом і відповіддю [5].

Механізм «відмітка часу» має на увазі реєстрацію часу для кожного повідомлення. У цьому випадку кожен користувач мережі визначає, наскільки «застаріло» отримане повідомлення, і вирішує не приймати його, оскільки воно може бути помилковим.

В обох випадках для захисту механізму контролю слід застосовувати шифрування, щоб бути впевненим, що відповідь відправлена не зловмисником.

При використанні відміток часу виникає проблема допустимого тимчасового інтервалу затримки для підтвердження автентичності сеансу: повідомлення з Timestamp (відмітка про час) в принципі не може бути передано миттєво. Крім того, комп'ютерний годинник одержувача і відправника не можуть бути абсолютно синхронізовані.

При порівнянні і виборі протоколів автентифікації необхідно враховувати наступні характеристики:

- наявність взаємної автентифікації. Це властивість відображає необхідність взаємної автентифікації між сторонами автентифікаційного обміну;
- обчислювальну ефективність. Це кількість операцій, необхідних для виконання протоколу;
- комунікаційну ефективність. Дана властивість відображає кількість повідомлень і їх довжину, необхідну для здійснення автентифікації;
- наявність третьої сторони. Прикладом третьої сторони може служити довірений сервер розподілу симетричних ключів або сервер, який реалізує дерево сертифікатів для розподілу відкритих ключів;
- гарантії безпеки. Прикладом може служити застосування шифрування і цифрового підпису.

Висновки:

Телефонний зв’язок на основі технології VoIP набуває все більшої популярності в нашій країні, але поряд з інформацією про його переваги, ми все частіше чуємо повідомлення про хакерські та хакерські атаки на телефонні послуги.

Так, ймовірність злому IP-телефонії вище, ніж традиційної, це заперечувати безглуздо. З іншого боку, приймати рішення про перехід на IP-телефонію правильніше не на підставі показника ймовірності злому, а на підставі співвідношення переваги / недоліки. Відзначимо, що технології VoIP базуються на технології IP і звідси можна зробити два висновки: якщо ваша локальна мережа має високий рівень безпеки, то і впроваджений сервіс IP-телефонії за замовчуванням буде добре захищений. Якщо інфраструктура має недоліки, то введення будь-якого додаткового сервісу провокує появу нових вразливостей.

Після проведеного аналізу, стає очевидним те що захист IP-телефонії може бути забезпечений тільки тоді, коли заходи безпеки застосовуються на всіх рівнях мережевої інфраструктури. По суті злом IP-телефонії - це така ж хакерська атака, як і в разі злому сайту або бази клієнтів, що використовує такі ж прийоми і методи. Тому за безпеку IP-телефонії, як і за безпеку всього в локальній мережі, повинен відповідати фахівець з мережевої безпеки, який повинен не забувати про основні способи захисту мережі:

4. Детальна побудова топології мережі.
5. Використання технологій автентифікації.
6. Використання методів криптографічного захисту.
7. Використання захисту від прослуховування.

РОЗДІЛ 3

РОЗГЛЯД ТА ПОРІВНЯННЯ ПРОТОКОЛІВ АВТЕНТИФІКАЦІЇ

3. Забезпечення безпеки з точки зору перевірки прав доступу до ресурсів (AAA)

AAA (Authentication Authorization and Accounting) - система автентифікації та обліку подій, вбудована в операційну систему Cisco IOS, яка забезпечує користувачам безпечний віддалений доступ до мережевого обладнання. Вона пропонує різні методи ідентифікації користувача, авторизації, а також збирання та відправлення інформації на сервер.

Мережа IP-телефонії будь-якого постачальника, як правило, має кілька точок доступу до послуги; з такою організаційною схемою не доцільно реалізовувати процес автентифікації користувача для кожної точки доступу окремо (на місці). Набагато розумніше централізувати процес автентифікації за допомогою окремого сервера та загальної бази даних, до якої звертатимуться сервери доступу (це рішення називається непрямою автентифікацією). Це пояснюється головним чином з точки зору адміністративних проблем, які виникають у разі організації організації автентифікації [6].

3.1. Непряма автентифікація

Непряма автентифікація - це модель, в якій механізм автентифікації розташований подалі від інших мережевих серверів, і вони спілкуються з ним щоразу, коли користувач запитує доступ.

Рішення непрямої автентифікації можуть впоратися з проблемами масштабування в центрах обробки даних, які мають одну групу користувачів,

але кілька точок обслуговування. Навіть на сайті, що має лише два сервери, буде важко підтримувати сумісність двох окремих баз даних автентифікації.

Якщо інші шаблони проектів забезпечують комбінацію механізмів автентифікації та контролю доступу, то шаблон непрямої автентифікації переміщує механізм автентифікації з точки обслуговування на окремий сервер автентифікації. Усі інші компоненти мережі надають послуги або контролюють доступ до ресурсів, але не приймають рішення про автентифікацію. Натомість вони аутентифікують користувачів опосередковано, звертаючись до сервера автентифікації, коли хтось намагається зареєструватися в системі [10].

З точки зору забезпечення безпеки з'єднання як в мережах IP-телефонії зокрема, так і в IP-мережах загалом, проблему можна умовно розділити на два компоненти.

Перша - проблема забезпечення законного та безпечного доступу до мережевих ресурсів та послуг, а друга - безпека інформації, яка вже знаходиться безпосередньо на каналах. Ця перша частина проблеми забезпечення безпеки в мережах IP-телефонії є предметом даної дипломної роботи.

Очевидно, що головна роль у вирішенні подібних проблем належить процесу автентифікації користувача. Завдяки структурі мультисервісної мережі, на основі якої надаються послуги IP-телефонії, ми будемо зацікавлені в непрямій автентифікації, її протоколах, а також слабких і сильних сторін.

Сьогодні багато широко відомих систем забезпечують непряму автентифікацію, використовуючи спеціально розроблені протоколи [9].

Відкритим стандартом для здійснення непрямої автентифікації є протокол RADIUS. Взагалі протокол непрямої автентифікації починається, коли хтось намагається зареєструватися в сервісному пункті з віддаленого місця, що може бути, наприклад, робочою станцією. Коли сервісний пункт отримує запит на реєстрацію, він пересилає ім'я користувача та пароль на сервер автентифікації. Часто для пересилання даних таких повідомлень

використовується внутрішній протокол, такий як RADIUS або протокол, розроблений виробником. Якщо сервер підтверджує автентифікацію, він надсилає в сервісну точку підтвердження, відформатованого відповідно до цього внутрішнього протоколу. Отримавши його, сервісний пункт приймає на виконання спробу користувача зареєструвати. Якщо сервер надсилає помилку, точка обслуговування відхиляє запит. Оскільки запити автентифікації переспрямовуються на сервер автентифікації, існує ризик, що зловмисник підробить повідомлення "Доступ надано", щоб обманути точку доступу; тому шифрування повинно використовуватися для автентифікації двосторонніх повідомлень між точкою обслуговування та сервером автентифікації.

Деякі системи, що використовують непряму автентифікацію, можуть мати високий рівень відмовостійкості, підтримуючи функцію переадресації. Якщо будь-який з серверів виходить з ладу (в тому числі під час атаки DOS), запити автентифікації можуть бути перенаправлені на альтернативний сервер, що містить копію всієї бази даних автентифікації. Це дозволяє постачальнику послуг IP-телефонії копіювати свої послуги на декількох хост-машинах та здійснювати автентифікацію на декількох серверах автентифікації, тим самим усуваючи появу критичної точки відмови [6].

3.2. Технології AAA на основі протоколу TACACS+

3.2.1. Протокол TACACS+

TACACS+ - це простий протокол контролю доступу, заснований на стандартах UDP, розроблених Bolt, Beranek і Newman, Inc. (BBN).

TACACS+ - це серверний додаток безпеки, який дозволяє на основі відповідного протоколу здійснювати централізований контроль доступу користувачів до послуг. Інформація про послуги та користувачів TACACS+ зберігається в базі даних, яка зазвичай знаходиться на комп'ютері під

управлінням UNIX або Windows NT. TACACS+ дозволяє використовувати єдиний сервер управління додатками для надання незалежної підтримки служб AAA.

Протокол TACACS+ працює за технологією клієнт-сервер, рис. 3.1.

Основним структурним компонентом протоколу TACACS є розділення автентифікації, авторизації та обліку. Це дозволяє обмінюватися ідентифікаційними повідомленнями будь-якої довжини та вмісту, а отже, використовувати будь-який механізм ідентифікації для клієнтів TACACS+, включаючи PPP PAP, PPP CHAP, апаратні картки тощо.

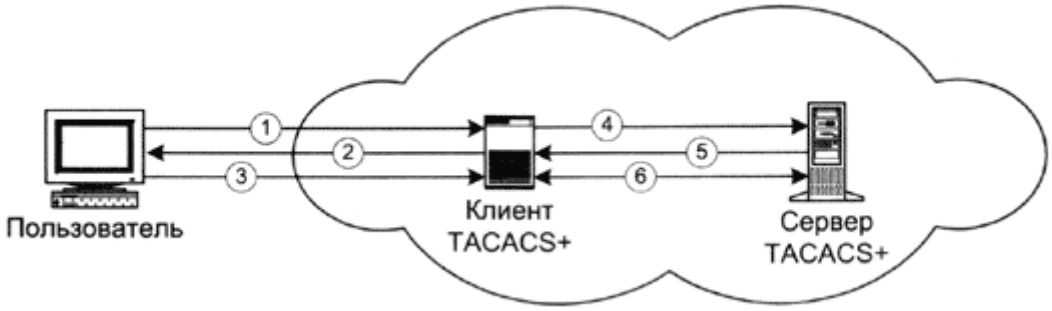

Рис. 3.1. Схема роботи мережі з сервером TACACS+

Авторизація - це процес визначення дій, дозволених даному користувачеві. Автентифікація зазвичай передує авторизації, але це не є необхідним. У запиті на авторизацію можна вказати, що автентифікацію користувача не проводили (ідентифікація користувача не доведена). У цьому випадку особа, відповідальна за авторизацію, повинна самостійно вирішити, чи дозволяти такого користувача до запитуваних послуг. Протокол TACACS+ дозволяє здійснювати лише позитивну чи негативну авторизацію, але цей результат дозволяє підлаштовуватися під потреби конкретного замовника. Авторизацію можна проводити на різних етапах, наприклад, коли користувач вперше входить до мережі та хоче відкрити графічний інтерфейс, або коли користувач запускає PPP та намагається використовувати IP-протокол із певною IP-адресою через PPP. У цих випадках демон сервера TACACS + може

дозволити надання послуг, але може встановити часові обмеження або вимагати список доступу IP для канала PPP [7].

3.2.2. Властивості протоколу TACACS+

TACACS+ підтримує такі функції сервера безпеки:

- TCP-пакети для надійної передачі даних. Використання TCP в якості протоколу зв'язку для TACACS+ з'єднань між сервером доступу та сервером безпеки. Для TACACS+ порт TCP 49 зарезервований.
- Архітектура AAA. Кожна послуга надається окремо і має власну базу даних, але, тим не менш, вони працюють разом як єдиний сервер захисту.
- Шифрування каналу. Частина пакету TCP, що містить дані протоколу TACACS+, шифрується з метою захисту трафіку між сервером доступу та сервером захисту.
- Кожен пакет TACACS+ має 12-байтовий заголовок, надісланий чітким текстом, і тіло змінної довжини, що містить параметри TACACS+. Тіло пакету шифрується за допомогою алгоритму з використанням псевдовипадкового заповнювача, отриманого за допомогою MD5. Пакети TACACS+ передаються по мережі та зберігаються сервером TACACS+ у зашифрованому вигляді. За необхідності пакет розшифровується сервером доступу та програмою TACACS+ шляхом реверсування алгоритму шифрування.
- Автентифікація PAP та CHAP. Він забезпечує повний контроль автентифікації за допомогою інструментів виклику / відповіді PAP та CHAP, а також за допомогою використання діалогових вікон введення пароля доступу та підтримки повідомлення процедури запуску інтерактивного сеансу.
- Захист локальних та глобальних мереж. Підтримка віддаленого та локальної мережі AAA для доступа до серверів доступу, маршрутизаторів та

іншого мережевого обладнання, що підтримує TACACS+. Це дозволяє централізоване управління мережевим обладнанням.

- Функція зворотного дзвінка. Ця функція повертає телефонні дзвінки, змушуючи сервер доступу викликати відповідного користувача, що може забезпечити додаткові гарантії безпеки.
- Індивідуальні списки доступу користувачів. База даних TACACS+ може доручити серверу доступу до мережі контролювати доступ користувача до мережевих служб та ресурсів під час фази авторизації на основі списку доступу [9].

3.2.3. Процеси AAA в протоколі TACACS+

Автентифікація не є обов'язковою. Вона розглядається як опція, яка налаштована на сайті. У деяких місцях це взагалі не потрібно, в інших місцях її можна використовувати лише для обмеженого набору послуг.

Заголовок пакету TACACS+ містить поле типу, яке вказує, що пакет є частиною процесу AAA. TACACS+ автентифікація розрізняє три типи пакетів: START (старт), CONTINUE (продовження) та REPLY (відповідь).

У запиті на авторизацію можна вказати, що автентифікацію користувача не проводили (ідентичність не доведена). У цьому випадку особа, відповідальна за авторизацію, повинна самостійно вирішити, чи дозволяти такого користувача до запитуваних послуг. Протокол TACACS+ дозволяє здійснювати лише позитивну чи негативну авторизацію, але цей результат дозволяє підлаштовуватися під потреби конкретного замовника.

Авторизація може здійснюватися на різних етапах, наприклад, коли користувач вперше входить до мережі та хоче відкрити графічний інтерфейс або коли користувач запускає PPP та намагається використовувати IP-протокол із певною IP-адресою через PPP. У цих випадках демон сервера

TACACS може дозволити надання послуг, але може встановити часові обмеження або вимагати список доступу IP для канала PPP.

Процес авторизації TACACS+ використовує два типи пакетів: REQUEST (запит) та RESPONSE (відповідь). Цей процес авторизації користувача керується за допомогою обміну парами атрибутів / значень між сервером безпеки TACACS + та сервером доступу [10].

Аудит (або облік) зазвичай слідкує після автентифікації та авторизації. Облік - це запис дій користувачів. У системі TACACS+ облік може виконувати два завдання. По-перше, його можна використовувати для перерахунку використовуваних послуг. По-друге, його можна використовувати в цілях безпеки. Для цього TACACS+ підтримує три типи облікових записів. Початкові записи вказують на те, що послугу потрібно запустити. Записи зупинки вказують на те, що послуга щойно закінчилася. Записи "оновлення" є проміжними і вказують на те, що послуга все ще надається. Облікові записи TACACS+ містять всю інформацію, яка використовується під час авторизації, а також інші дані: час початку та закінчення (за необхідності) та дані про використання ресурсів. Транзакції між клієнтом TACACS+ та сервером TACACS+ ідентифікуються за допомогою загального "секрету", який ніколи не передається по каналах зв'язку. Зазвичай цей «секрет» встановлюється вручну на сервері та на клієнті. TACACS+ може бути налаштований для шифрування всього трафіку, який передається між клієнтом та демоном сервера TACACS+ [6].

Під час процесу аудиту TACACS+ використовує два типи пакетів - REQUEST (запит) та RESPONSE (відповідь). Цей процес схожий на процес авторизації. Під час процесу аудиту створюються записи з інформацією про діяльність користувачів щодо визначених послуг. Дії запису записів, що виконуються мережевим обладнанням, можуть зберігатися в певному стандартному форматі на сервері захисту з метою подальшого аналізу.

Згідно з TACACS+, аудит AAA не є надійним засобом захисту і зазвичай використовується лише для цілей бухгалтерського обліку та управління.

Однак за допомогою аудиту AAA можна контролювати дії користувача, щоб, наприклад, помітити його незвичну поведінку під час роботи з мережевим обладнанням [10].

3.3. Технології AAA на основі протоколу RADIUS

3.3.1. Протокол RADIUS

Протокол RADIUS був розроблений компанією Livingston Enterprises, Inc. (нині є частиною Lucent Technologies) як протокол автентифікації доступу до сервера та обліку. В даний час протокол RADIUS описаний в RFC 2865, а аудит RADIUS в RFC 2866.

RADIUS (Remote Access Dial-In User Service - служба користування віддаленим доступом) являється розподіленим протоколом, що використовується в рамках технології клієнт / сервер і який захищає мережу від несанкціонованого доступу. Наприклад, Cisco підтримує RADIUS як частину системи безпеки AAA.

Протокол, про який йдеться, поєднує автентифікацію та авторизацію, а не розглядає їх окремо, як це робить в відношенні аудиту [8].

Протокол RADIUS можна використовувати з іншими протоколами безпеки AAA, такими як TACACS+, Kerberos та локальними базами даних безпеки. Протокол RADIUS реалізований у багатьох мережевих середовищах, які потребують високого рівня захисту, за умови підтримки доступу до мережі для віддалених користувачів. Це повністю відкритий протокол, що постачається у вихідному текстовому форматі, який можна змінити, щоб він міг працювати з будь-якою доступною на даний момент системою захисту. Широка популярність RADIUS забезпечується можливістю додавання нових пар атрибутів / значень на додаток до описаних у RFC 2865. У протоколі RADIUS є атрибут постачальника, який дозволяє постачальнику підтримувати

власні розширені набори атрибутів, включаючи нестандартні атрибути. Через використання пар атрибутів / значень конкретних постачальників може бути важко інтегрувати продукти безпеки сервера RADIUS в інші системи безпеки. Сервери безпеки RADIUS та пов'язані з ними клієнти повинні ігнорувати нестандартні пари атрибутів / значень, створені конкретними постачальниками.

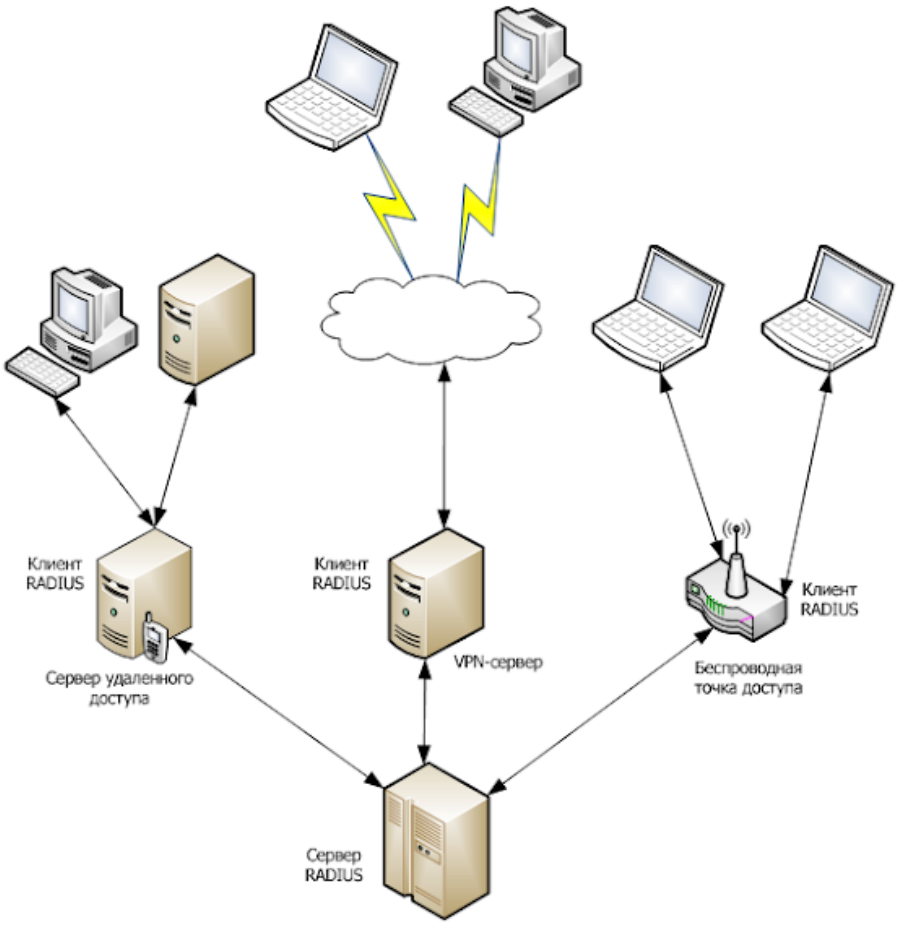

Рис. 3.2 Топологія мережі з використанням серверу RADIUS

Зв'язок між NAS та сервером RADIUS базується на протоколі UDP. Взагалі вважається, що протокол RADIUS не пов'язаний із з'єднанням. Усі проблеми, пов'язані з доступністю сервера, повторною передачею даних та відключеннями після закінчення тайм-ауту, контролюються пристроями, що працюють за протоколом RADIUS, але не самим протоколом передачі. Протокол RADIUS заснований на технології клієнт-сервер, рис 3.2. Клієнтом RADIUS зазвичай є NAS, а сервер RADIUS вважається "демоном", що працює

на машині UNIX або NT. Клієнт передає інформацію про користувачів конкретним серверам RADIUS, а потім діє відповідно до інструкцій, отриманих від сервера. Сервери RADIUS приймають запити на з'єднання користувачів, підтверджують автентифікацію користувачів, а потім надсилають всю інформацію про конфігурацію, необхідну клієнту для обслуговування користувача.

Для інших серверів RADIUS або інших типів серверів ідентифікації сервер RADIUS може виступати як проксі-клієнт [9].

3.3.2. Властивості і можливості протоколу RADIUS

RADIUS підтримує такі функції сервера безпеки:

- UDP-пакети. Для зв'язку RADIUS між сервером доступу та сервером захисту використовується протокол UDP та UDP-порт 1812, офіційно призначений для цього. Деякі реалізації RADIUS використовують порт UDP 1645. Використання UDP спрощує реалізацію клієнта та сервера RADIUS.
- Поєднання автентифікації та авторизації та виділення аудиту. Сервер RADIUS отримує запити користувачів, виконує автентифікацію та надає клієнту інформацію про конфігурацію. Аудит виконується сервером аудиту RADIUS.
- Шифрування паролів користувачів. Паролі, що містяться в пакетах RADIUS (і це лише паролі користувачів), шифруються за допомогою хешування MD5.

- Автентифікація PAP та CHAP. Забезпечує контроль автентифікації за допомогою інструментів PAP та CHAP для виклику / відповіді, а також через діалогове вікно для запуску сеансу та введення пароля, наприклад, входу в систему UNIX

- Захист WAN. Забезпечує підтримку віддаленого доступу AAA для серверів доступу багатьох постачальників, які підтримують клієнтів RADIUS. Забезпечує можливість централізації управління віддаленим доступом.
- Підтримка ряду протоколів, що забезпечують доступ терміналу до сервера безпеки RADIUS.
- Функція зворотного дзвінка. Ця функція повертає телефонні дзвінки, змушуючи сервер доступу зателефонувати відповідному користувачеві, що може забезпечити додаткові гарантії безпеки для користувачів, які використовують доступ до телефонної лінії.
- Розширюваність. Усі транзакції передбачають використання пар атрибутів / значень змінної довжини. Нові атрибути можуть бути додані до існуючих реалізацій протоколу.
- Гарантована безпека мережі. Автентифікація транзакцій між клієнтом та сервером захисту RADIUS передбачає використання загального секретного значення [10].

3.3.3 Процес автентифікації і авторизації в протоколі RADIUS

Клієнт RADIUS та сервер безпеки RADIUS обмінюються пакетами Access-Request (доступ-запит), Access-Accept (доступ-підтвердження), Access-Reject (доступ-відмова) та Access-Challenge (доступ-виклик). Як показано на рис. 3.3, при спробі підключитися до сервера доступу до мережі, який має конфігурацію клієнта RADIUS, виконуються наступні дії:

1. Користувач ініціює запит автентифікації PPP на сервер мережевого доступу.
2. Користувачу пропонується ввести ім'я користувача та пароль
3. Сервер доступу до мережі надсилає серверу захисту RADIUS пакет-запит доступу, що містить ім'я користувача, зашифрований пароль та інші атрибути.

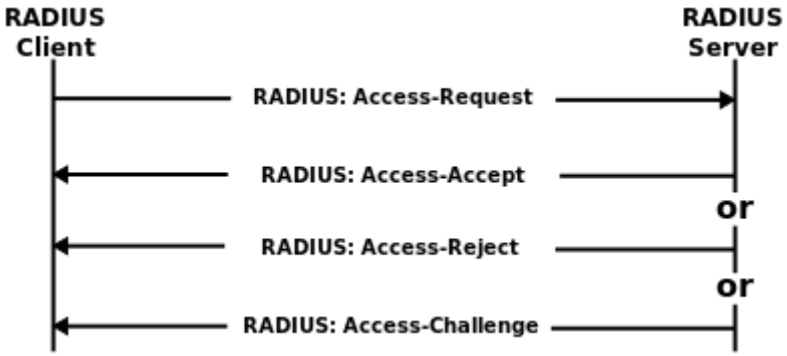

Рис. 3.3. Процес автентифікації в протоклі RADIUS

4. Сервер безпеки RADIUS ідентифікує ініціюючого клієнта, аутентифікує користувача, перевіряє параметри авторизації користувача та повертає один із наступних відповідей:

1) Access-Accept - користувач має автентифікацію.

2) Access-Reject - користувач не має автентифікації, і сервер мережевого доступу або пропонує знову ввести ім'я користувача та пароль, або забороняє доступ.

3) Access-Challenge - виклик є додатковою особливістю сервера безпеки RADIUS.

5. Сервер мережевого доступу отримує доступ до параметрів автентифікації, які дозволяють використовувати певні послуги.

6. Відповідь Access-Accept або Access-Reject асоціюється з додатковими даними (парами атрибутів / значень), що використовуються для сесій EXEC та авторизації. Процес автентифікації RADIUS повинен бути завершений на початку процесу авторизації [8].

7. Сервер безпеки RADIUS може періодично надсилати пакети Access-Challenge на сервер мережевого доступу, щоб вимагати від користувача повторного введення імені користувача та пароля, інформування про стан сервера мережевого доступу або виконання деяких інших дій, передбачених

розробниками RADIUS сервер. Клієнт RADIUS не може надсилати пакети Access-Challenge.

3.3.4 Процес аудиту на основі протоколу RADIUS

Протокол RADIUS був удосконалений, щоб забезпечити доставку аудиторської інформації від клієнта RADIUS на сервер аудиту RADIUS через порт UDP 1813. Клієнт RADIUS несе відповідальність за надсилання інформації про аудит користувача на відповідний сервер аудиту RADIUS, для використовується пакет типу Accounting-Request (аудит-запит) з відповідним набором пар атрибутів / значень. Сервер аудиту RADIUS повинен прийняти запит аудиту та повернути відповідь, що підтверджує успішне отримання запиту. Для цього використовується пакет типу Accounting-Response (аудит-відповідь).

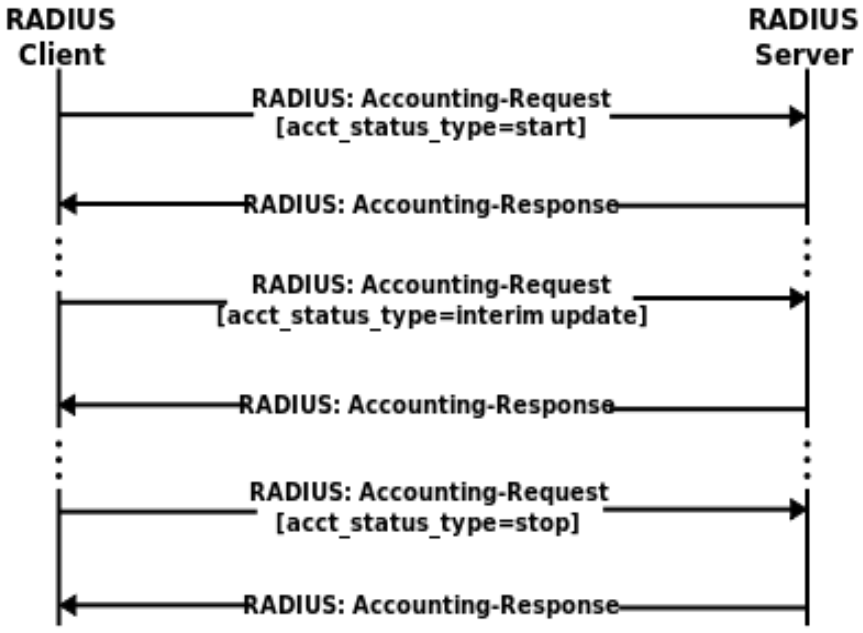

Рис. 3.4. Процес аудиту на основі протоколу RADIUS

Як видно з рис. 3.4., коли ви намагаєтеся підключитися до сервера мережевого доступу, який має конфігурацію клієнта RADIUS, виконуються наступні дії:

1. Після первинної автентифікації сервер доступу до мережі надсилає пусковий пакет Accounting-Request на сервер безпеки RADIUS.
2. Сервер безпеки RADIUS підтверджує отримання стартового пакету, повертаючи пакет Accounting-Response.
3. Наприкінці використання послуги сервер доступу до мережі надсилає стоп-пакет Accounting-Request; Цей пакет вказує тип наданої послуги та додаткову статистику.
4. Сервер безпеки RADIUS підтверджує отримання пакету зупинки, повертаючи пакет Accounting-Response.

3.4. Порівняння протоколів TACACS+ и RADIUS

Хоча TACACS+ і RADIUS дуже схожі за функціональністю, вони мають кілька важливих відмінностей, як зазначено в табл. 3.1.

Таблиця 3.1.

Порівняння протоколів автентифікації TACACS+ та RADIUS

Функціональні можливості	TACACS+	RADIUS
Підтримка AAA	Поділ трьох сервісів AAA	Автентифікація і авторизація об'єднуються, а аудит відділяється

Транспортний протокол	TCP	UDP
Обмін повідомленнями між клієнтом і сервером захисту	Двонаправлений	Однонаправлений
Підтримка протоколів віддаленого і міжмережевого доступу	Повна підтримка	Відсутня підтримка NetBEUI
Цілісність даних	Шифрується весь пакет TACACS	Шифруються тільки паролі користувачів
Можливість перенаправлення запиту	Відсутня	Присутня

Крім того, TACACS+ підтримує двонаправлений потік виклику / відповіді між серверами мережевого доступу, аналогічно тому, як це робиться в CHAP. RADIUS підтримує однонаправлений виклик / відповідь з сервера безпеки RADIUS клієнту RADIUS [10].

Цілісність даних. TACACS+ передбачає шифрування вмісту пакетів. RADIUS шифрує лише атрибути пароля в пакеті Access-Request. Це означає кращу захищеність TACACS+.

Крім того, порівнюючи TACACS + і RADIUS, можна зазначити наступне:

- Параметри налаштування. Гнучкість протоколу TACACS+ забезпечує можливість налаштування багатьох параметрів для задоволення індивідуальних потреб користувачів. Через відсутність гнучкості RADIUS, багато функцій, доступних під TACACS +, недоступні при використанні RADIUS (наприклад, каталоги повідомлень). Однак RADIUS підтримує можливість змінювати набори пар атрибут / значення.

- Процес авторизації. Під час використання TACACS+ сервер приймає або відхиляє запит автентифікації на основі інформації профілю користувача. Вміст профілю користувача залишається невідомим клієнту (NAS). У системі RADIUS всі атрибути профілю користувача, що надсилаються з відповіддю, передаються на сервер мережевого доступу. Сервер приймає або відхиляє запит на автентифікацію на основі значень атрибутів, які він отримує.

- За великим рахунком, протокол RADIUS не підтримує авторизацію. Тобто, має сенс використовувати RADIUS лише там, де заздалегідь відомо, яку послугу надає конкретний клієнт RADIUS. TACACS + має підтримку авторизації. Але слід зазначити, що кількість дозволених сервісів досить обмежена в поточному. Тобто, для доступа до послуги RADIUS обробляє один запит (автентифікація - запит, відповідь), а TACACS+ - два (автентифікація та авторизація), але в той же час, використовуючи TACACS+, можна отримати доступ до іншої послуги.

- Аудит TACACS+ передбачає використання обмеженої кількості інформаційних полів. Аудит RADIUS може надати більше інформації, ніж можна отримати з аудиторських записів TACACS+, що є головною перевагою перед TACACS+.

- Можливість перенаправлення запиту. TACACS+ просто не має цієї функції. Протокол RADIUS має таку можливість. Це дуже суттєва перевага цього протоколу, якщо в інших регіонах є представництва оператора IP-телефонії. У цьому випадку клієнт, перебуваючи в іншому регіоні, набирає код доступу (номер та PIN-код). Далі локальний сервер RADIUS перенаправляє запит у відповідний регіон.

Проходить автентифікація і відповідь надсилається назад. Таким чином, RADIUS дозволяє розробити гнучку розподілену RADIUS схему. Отже, клієнт RADIUS на будь-який запит повинен чекати відповідь від сервера деякий час (тайм аут) і, якщо ні, знову надіслати пакет. Клієнт TACACS+ також повинен

завжди чекати відповіді від сервера, але на відміну від клієнта RADIUS, за відсутності відповіді, пакет не надсилається знову. Гарантія доставки забезпечується тим, що для обробки будь-якого запиту TACACS+ сервер і клієнт повинні встановити TCP-з'єднання (навіть якщо весь процес буде складатися з відправки та отримання 2 невеликих пакетів), і з точки зору часу - це досить тривалий процес (відповідно до цього, TACACS+ є за визначенням відносно повільним). Виходячи з цього, можна сказати, що RADIUS буде ефективнішим у мережі, де відсоток втрачених пакетів становить менше 5-10%; в інших мережах краще використовувати TACACS +. З цієї причини в мережах IP-телефонії, де необхідна продуктивність, зазвичай використовується протокол RADIUS [7].

3.5 Характеристика протоколів TACACS та RADIUS

Існує велика кількість відмінностей між протоколами RADIUS і TACACS +, але функції, які вони виконують, по суті однакові. Стандартний протокол RADIUS використовує протокол UDP на транспортному рівні. Протокол TACACS+, будучи приватною розробкою, використовує протокол TCP на транспортному рівні. Протокол RADIUS добре працює лише в середовищах IP, в той час як протокол TACACS+ корисний у середовищі з багатьма протоколами. В даний час протокол RADIUS підтримує більше атрибутів і дозволяє передавати більше інформації клієнту та серверу, ніж протокол TACACS+. Нарешті, RADIUS шифрує лише пароль, надісланий між клієнтом та сервером, тоді як TACACS+ шифрує всю надіслану інформацію.

Якщо мережа значною мірою неоднорідна, краще вибрати протокол RADIUS, оскільки він підтримується багатьма провайдерами. Якщо в мережі використовуються в основному пристрої Cisco, то, швидше за все, протокол TACACS+ стане правильним рішенням.

Часто виникає завдання перевірити користувача, перш ніж надати йому доступ до певних ресурсів. Ця перевірка називається cut-through proxy.

Ця послуга використовує інфраструктуру AAA (автентифікація, авторизація, облік) [10].

TACACS+ - протокол TCP / 49. Він має окремі запити на автентифікацію, авторизацію та облік. Через окремий запит на авторизацію він дозволяє враховувати та перевіряти всі введені команди. Не розширювані варіанти, слабкий «облік». Зазвичай використовується для адміністративного доступу.

RADIUS - це стандартний протокол. Працює над UDP / 1645,1646 або UDP / 1812,1813. Один новий, другий старий стандарт. Перший порт використовується для запиту автентифікації та відповіді, в якому одночасно передаються атрибути авторизації користувача, якщо такі є. Другий - для обліку (як правило, за допомогою RADIUS вони враховують передані пакети, враховують трафік та деякі системні параметри)

Таким чином, з автентифікацією все просто: якщо ви нічого іншого не вкажете, то користувачеві, а точніше, IP-адресі його комп’ютера стане можливим все.

Набагато цікавішим моментом є авторизація, тобто обмеження прав користувачів.

Використовуючи протокол TACACS+, ви можете обмежити доступ до певних ресурсів (мереж та протоколів), однак формат такого обмеження досить дивний: на сервері описуються всі такі протоколи і мережі, і поводження з ASA на сервер йде всякий раз, коли з'являється ще раніше не вивчений пакет.

Для цього потрібно окремо написати команду для авторизації. Ви можете використовувати той самий список доступу, який був використаний для автентифікації, або ви можете написати новий.

Простіше використовувати протокол RADIUS, який забезпечує можливість передачі рядків списку доступу в атрибутах користувача, який застосовується безпосередньо до користувача. Не потрібно писати додаткових команд. Правда, ці можливості має cisco ACS (сервер управління доступом). Я не знаю точно, чи існують безкоштовні та безкоштовні реалізації сервера RADIUS, які також можуть передавати рядки.

Зрозуміло, що облік не може здійснюватися на сервері LOCAL (локально), а також на сервері LDAP. Не так багато атрибутів передається TACACS, як нам би хотілося, але RADIUS краще підходить. І ви можете використовувати будь-який. Зокрема, коли налаштовується автентифікація та авторизація через LDAP для обліку, то використовується IAS (це саме RADIUS, вбудований у сервері Windows). Однак видаляти з нього звіти не так зручно, як з ACS або інших, більш адаптованих рішень [6].

Зовнішня автентифікація в цьому випадку cisko не знає користувачів; логін завжди перевіряється на зовнішньому сервері за допомогою протоколу TACACS+ або RADIUS (більш поширений). Недоліки очевидні: є необхідність у додатковій організації та підтримці сервера RADIUS, і якщо вона недоступна, доступ до мережі буде відмовлено. Однак при масштабуванні системи додаються нові сервери доступу або резервні сервери RADIUS [8].

Висновки:

Рішення непрямої автентифікації використовуються, коли в системі є кілька точок обслуговування та коли важко підтримувати сумісність декількох окремих баз даних для автентифікації користувача. Для таких схем потрібен спеціальний сервер автентифікації в системі.

Усі інші сервісні точки опосередковують принципів опосередковано, звертаючись до сервера автентифікації, коли хтось намагається зареєструватися в системі.

Відкритим стандартом для здійснення непрямої автентифікації є протоколи Radius та TACACS+ розроблений Cisco.

Виходячи з порівняння цих протоколів можна констатувати факт, що для забезпечення кращої безпеки слід будувати мережу використовуючи технологію AAA з використанням протоколу TACACS+.

ЗАГАЛЬНІ ВИСНОВКИ ПО РОБОТІ

У даній дипломній роботі були розглянуті проблеми IP-телефонії та її проблеми в безпеці. Було розглянуто рівні архітектури IP-телефонії, побудова мереж на основі протоколів H.323, SIP та MGCP; сценарії систем «клієнт-клієнт», «клієнт-сервер». Розглянуто види загроз IP-телефонії, такі як реєстрація чужого терміналу, що дозволяє робити дзвінки за чужий рахунок, підміну абонента, внесення змін до голосового або сигнального трафіку, зниження якості голосового трафіку, перенаправлення голосового або сигнального трафіку, перехоплення голосового або сигнального трафіку, підробка голосових повідомлень, завершення сеансу зв'язку, відмова в обслуговуванні і віддалений несанкціонований доступ до компонентів інфраструктури IP-телефонії. Ці проблеми запропоновано вирішувати різними способами: криптографії, захищеності каналу, технології AAA.

У даній дипломній роботі на основі технології AAA порівняно протоколи автентифікації TACACS+ і RADIUS. Після дослідження протоколів автентифікації, однією з основних складових захищеності, зроблено висновок, що в адміністративних мережах для захисту інформації краще використовувати протокол TACACS+, враховуючи особливості кожної мережі. Для мережі більшого масштабу краще використовувати протокол RADIUS.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Гольдштейн Б.С, Пінчук А.В., Суховицький А.Л. IP-телефонія
2. Джонатан Девідсон, Джеймс Пітерс, Манож Бхатія, Сатиш Калідінді, Судіпто М. Основи передачі голосових даних по мережах IP (IP Voice over IP Fundamentals).
3. Передачі голосових даних в реальному часі через інтернет протокол / Режим доступу до ресурсу: http://inmad.vntu.edu.ua/portal/static/E3E35C35-800E-48F9-A804-4DD5DB290AF0.pdf.
4. Phishing Activity Trends Report 2nd Quarter 2019 / Режим доступу до ресурсу: https://docs.apwg.org/reports/apwg_trends_report_q2_2019.pdf.
5. Взаємна перевірка справжності користувачів / Режим доступу до ресурсу: http://um.co.ua/9/9-4/9-48981.html.
6. Интернет решения / Режим доступу до ресурсу: http://www.gelios.biz/articles/ip-telefoniya-nastoyashhee-i-budushhee.html.
7. Стоп вирус / Режим доступу до ресурсу: http://www.stopvirus.kz/index.php.
8. Проект объединения независимых сетей VoIP / Режим доступу до ресурсу: http://voipx.ru/cgi-bin/loscont.cgi?ID=08.
9. IP-телефония / Режим доступу до ресурсу: http://www.ctspi.ru/TechSupp/ IPTEL/Obzor.htm.
10. Современные технологии / Режим доступу до ресурсу: http://www.telda.ru/ connection.html.