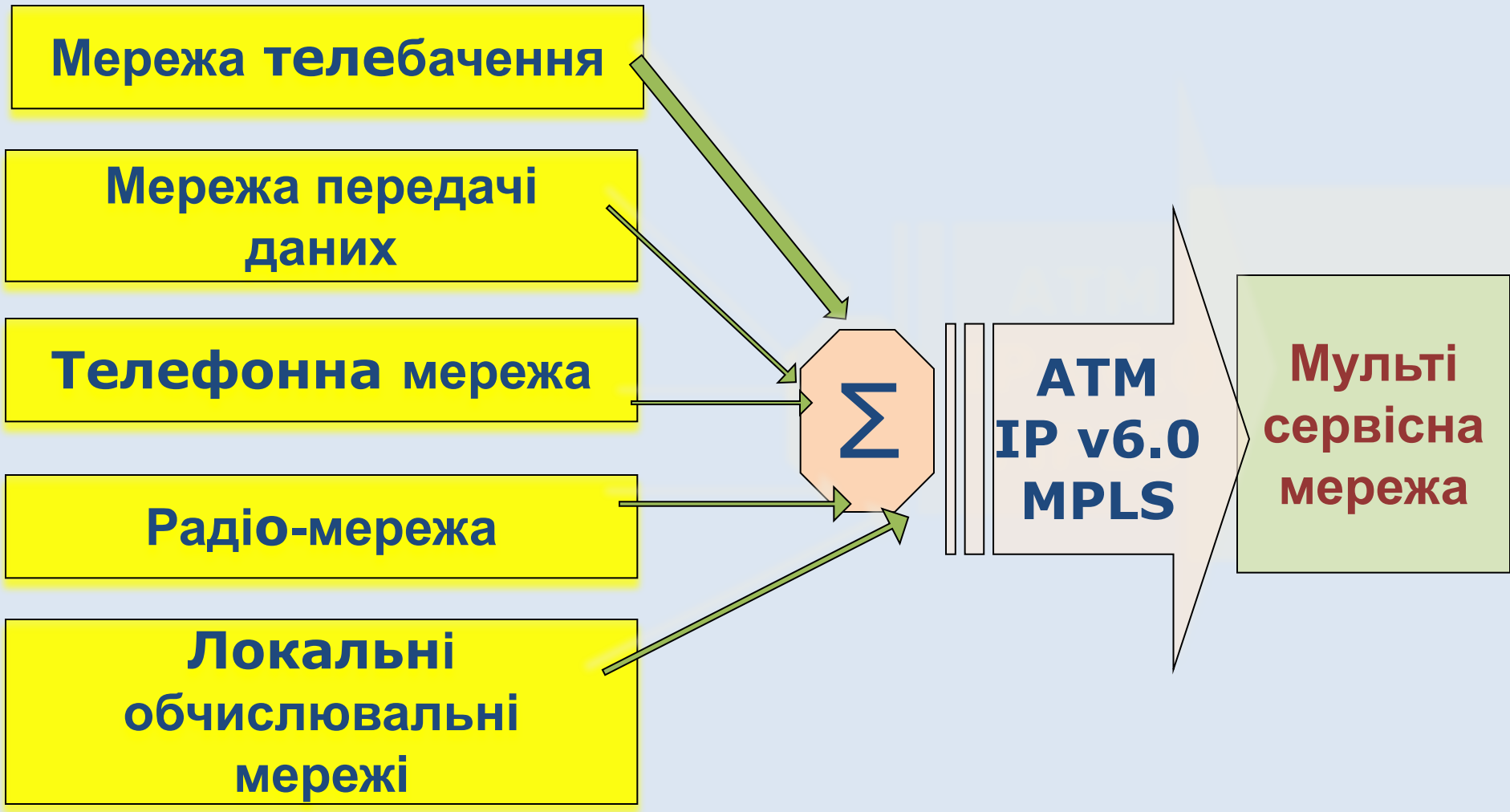
Захист інформації в інформаційно-комунікаційних системах

Лекція 15

Якість обслуговування –

Безпека NGN

Тенденції розвитку ІКС



MPLS (англ. Multiprotocol Label Switching — мультіпротокольна комутація по мітках) — механізм передачі даних, який емулює різні властивості мереж з комутацією каналів по мережах з комутацією пакетів.

Особливості сучасних ІКС

Інтеграція послуг користувача у єдину точку доступу

Мобільний доступ користувача до послуг

Гарантія якості наданих послуг

Інформаційна безпека телекомунікаційних послуг

Для досягнення комплексного рішення у середовищі з багатьма постачальниками **мережева безпека** повинна бути розроблена на основі стандартної архітектури захисту

Який захист необхідний і від яких загроз?
Які саме мережеві засоби та обладнання повинні бути захищені?
Які саме типи мережевої активності повинні бути захищені?

Недоліки традиційних мереж

Канали з часовим мультиплексуванням (TDM) проектуються з урахуванням найбільш несприятливій ситуації - пікового навантаження.
Протоколи ОКС7 вимагають, щоб у штатній ситуації завантаженість TDM-каналів не перевищувала 40%.
На практиці їх середнє завантаження становить 20-30%.
Додавання кожного нового елементу вимагає організації каналу "точка-точка" і поновлення маршрутних таблиць, а значить, додаткових капітальних та експлуатаційних витрат

ЕКОНОМІЯ :
- економія на капітальних витратах до 70%;
- економія на організації каналів доступу 60-80%;
- економія на поточному обслуговуванні та ремонті мережі до 50%;

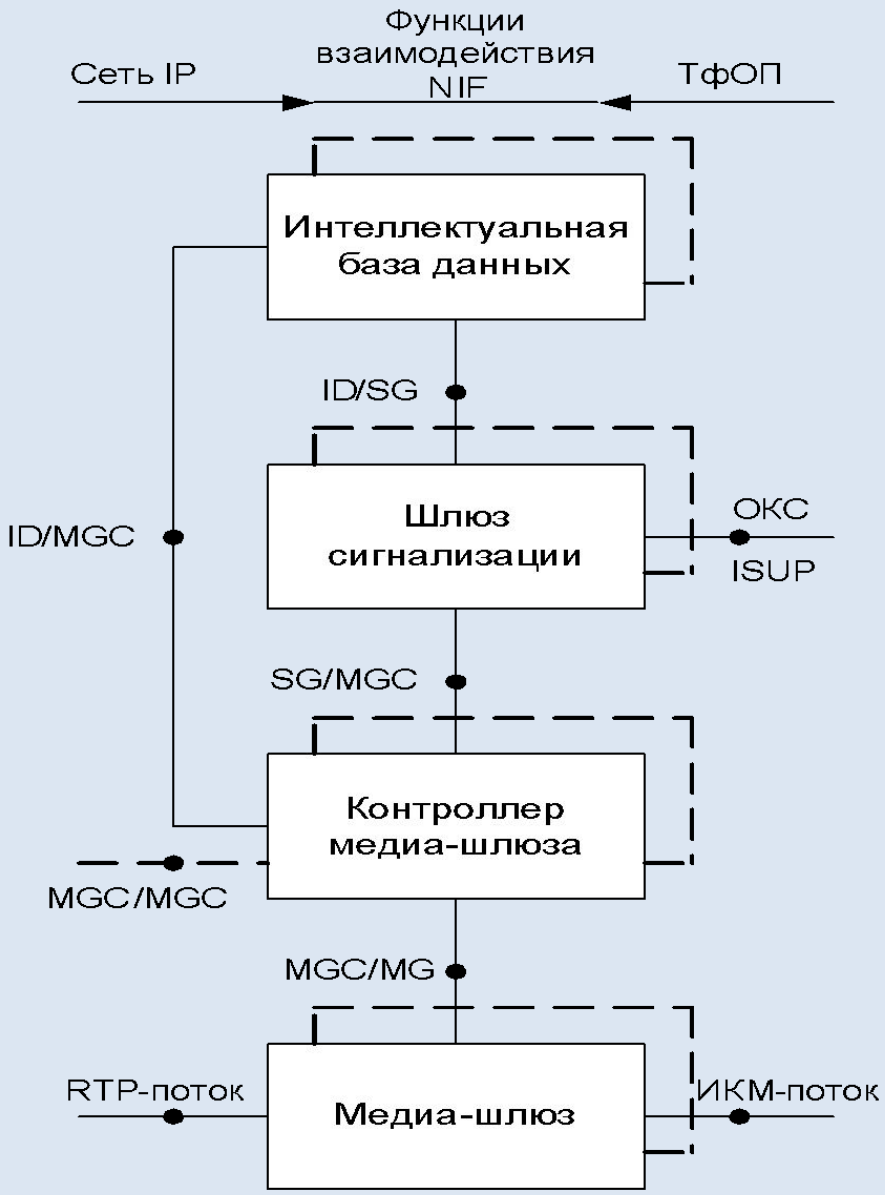
Мережі NGN

Мережі NGN базуються на інтернет-технологіях, що включають в себе IP-протокол і технологію MPLS.
На сьогодні розроблено кілька підходів до побудови мереж IP-телефонії, запропонованих організаціями ITU-T та IETF

Ключові особливості мереж NGN

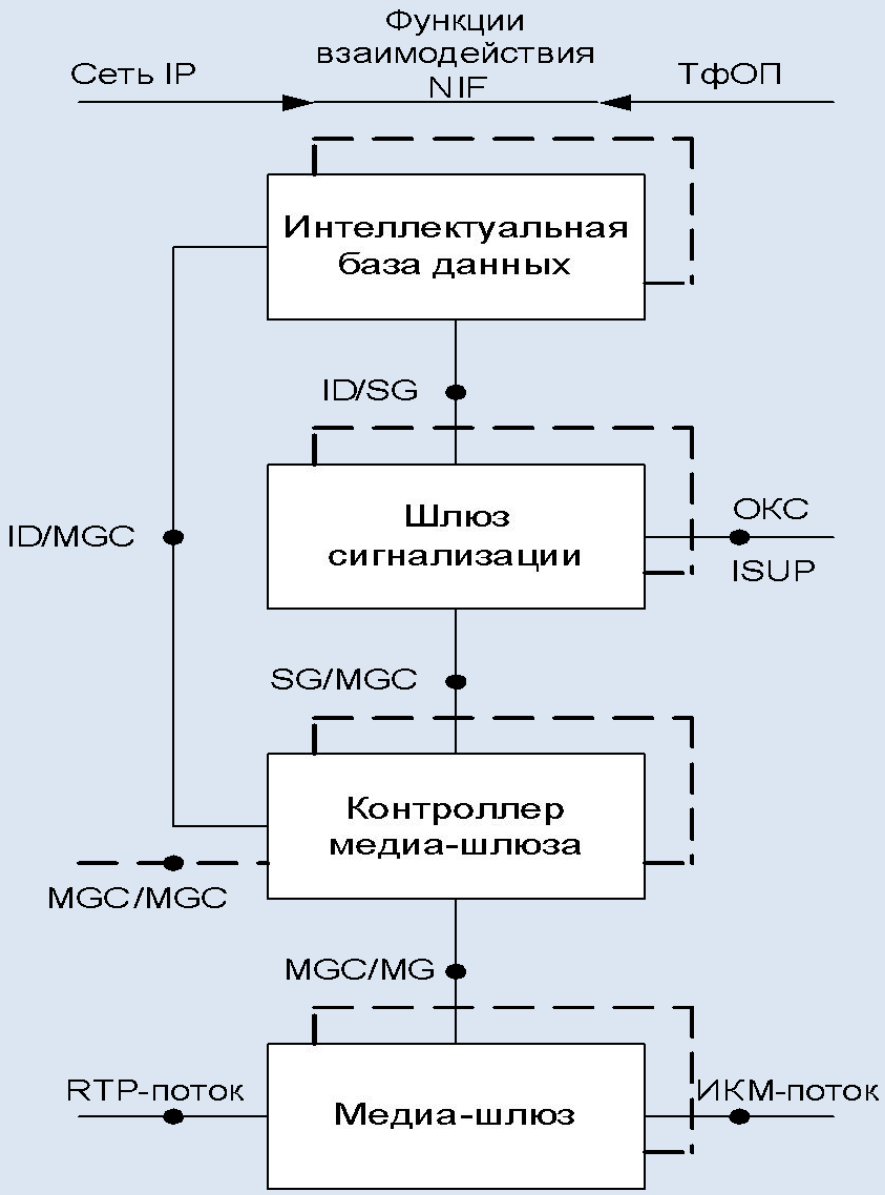
- використання в транспортній мережі пакетних технологій для передачі всіх видів інформації;
- застосування систем комутації з розподіленою архітектурою;
- відокремлення функцій підтримки послуг від комутації та передачі;
- забезпечення можливості широкосмугового доступу для будь-якого користувача;
- реалізація функцій експлуатаційного управління (у тому числі делегованих користувачам) за рахунок веб-технології

Архитектура NGN (рек. Y.1001)



Медіа-шлюз виконує функції перетворення інформаційних потоків.
RTP-потік формується при використанні транспортного протоколу реального часу (Real-Time Transport Protocol)
Потік, утворений системою передачі з **імпульсно-кодовою модуляцією** (ІКМ).
Медіа-шлюз повинен мати велику продуктивність.
Медіа-шлюз управляється контролером - **MGC (Softswitch)**.
Контролери можуть бути пов'язані між собою.
Контролер взаємодіє з інтелектуальної базою даних (**Intelligent ID** баз даних).

Архитектура NGN (рек. Y.1001)



Шлюз сигналізації (SG).
У бік ТфОП (мережі) шлюз сигналізації передає і приймає інформацію по мережі загальних каналів сигналізації (**ОКС**) (**SS**).
У мережі ОКС застосовується підсистема користувача ЦСІО – **ISUP** (встановлення з'єднання).
Взаємодія з контролером MGC здійснюється через інтерфейс, позначений як SG / MGC.
Для зв'язку з інтелектуальної базою даних визначений інтерфейс ID/SG.
Для підтримки послуг IC використовується прикладний протокол інтелектуальної мережі - INAP.

Рівнева архітектура (Lucent Technologies)

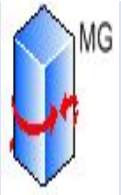
Рівень послуг мережі
Network service layer

Рівень керування
Control layer

Рівень середовища обміну даних
Media layer

Рівень доступу та транспорту
Access and transport layer

Абоненти ІКС



Рівень послуг забезпечує
- **функції користувача**, що передають пов’язані з послугами дані і
- **функції керування** (сигналізацію і контроль) та менеджмент ресурсів послуг і ресурсів мережі.

Розглядаються ті застосунки (їх послуги), які функціонують між p2p об’єктами.

послуги можуть відноситись до аудіо, даних або відео, окремо або в деякій комбінації.

Рівень управління (Control layer)

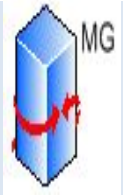
Рівень послуг мережі
Network service layer

Рівень керування
Control layer

Рівень середовища обміну даних
Media layer

Рівень доступу та транспорту
Access and transport layer

Абоненти ІКС



Рівень керування

-функції з керування всіма процесами в ІКС,

-нарахування плати за послуги зв'язку та технічну експлуатацію.

Для реалізації функцій - **Softswitch.**

Функції управління послугами: (автентифікація користувача, ідентифікація користувача, управління доступом до послуги, функції сервера застосувань)

Функції управління мережевим транспортом: (управління доступом до мережі, управління ресурсами/політикою мережі, забезпечення діючих з'єднань).

Рівень середовища обміну інформацією (Media layer)

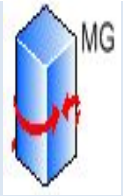
Рівень послуг мережі
Network service layer

Рівень керування
Control layer

Рівень середовища обміну даних
Media layer

Рівень доступу та транспорту
Access and transport layer

Абоненти ІКС



Рівень середовища обміну інформацією
- встановлення з'єднань між користувачами мережі
-міжмережеву взаємодію.

Типовим прикладом устаткування, яке реалізує ці функції в мережі NGN, служать апаратно-програмні засоби Media Gateway (медіа-шлюз).

Рівень доступу та транспорту (Access and transport layer)

Рівень послуг мережі
Network service layer

Рівень керування
Control layer

Рівень середовища обміну даних
Media layer

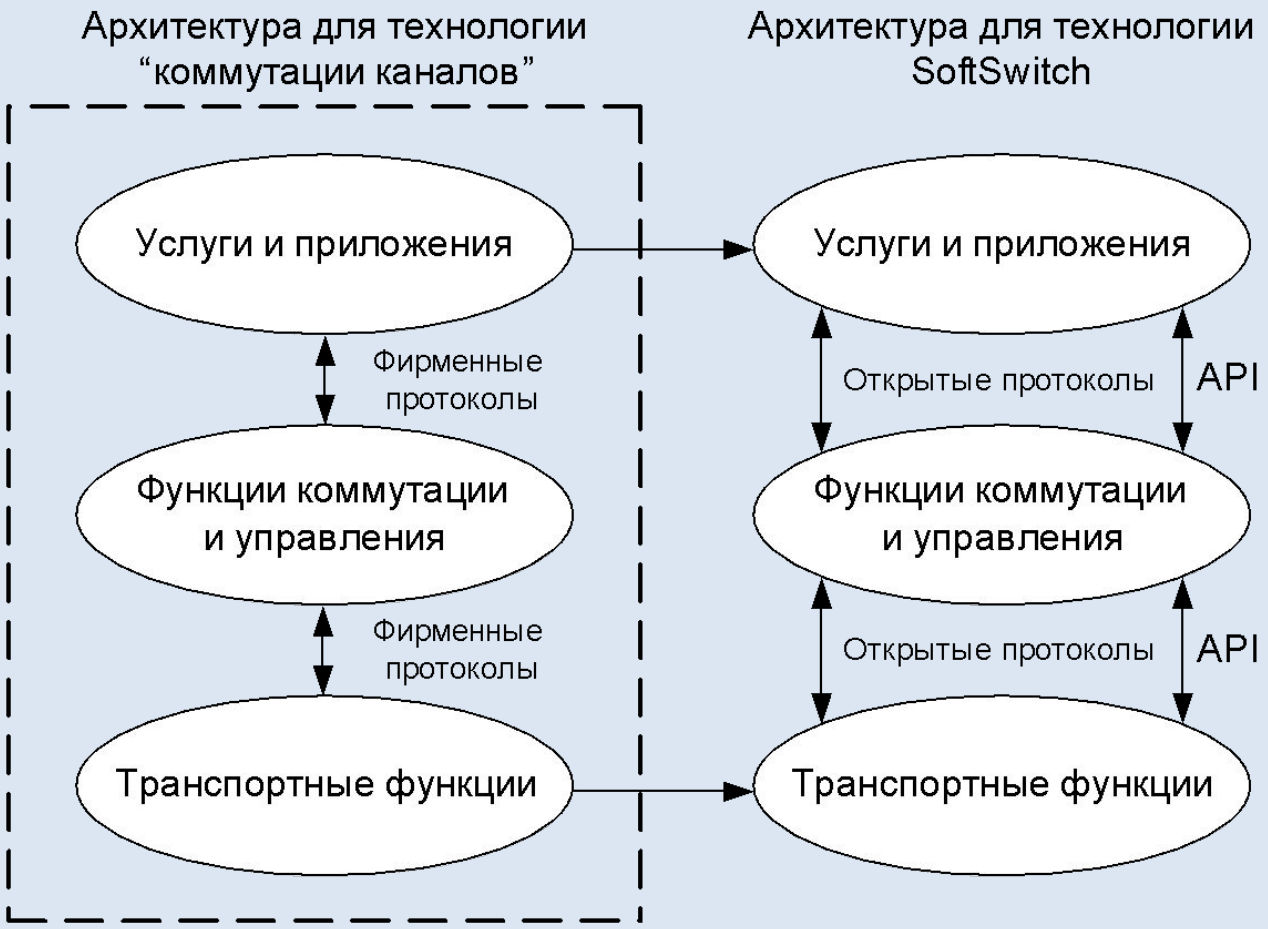
Рівень доступу та транспорту
Access and transport layer

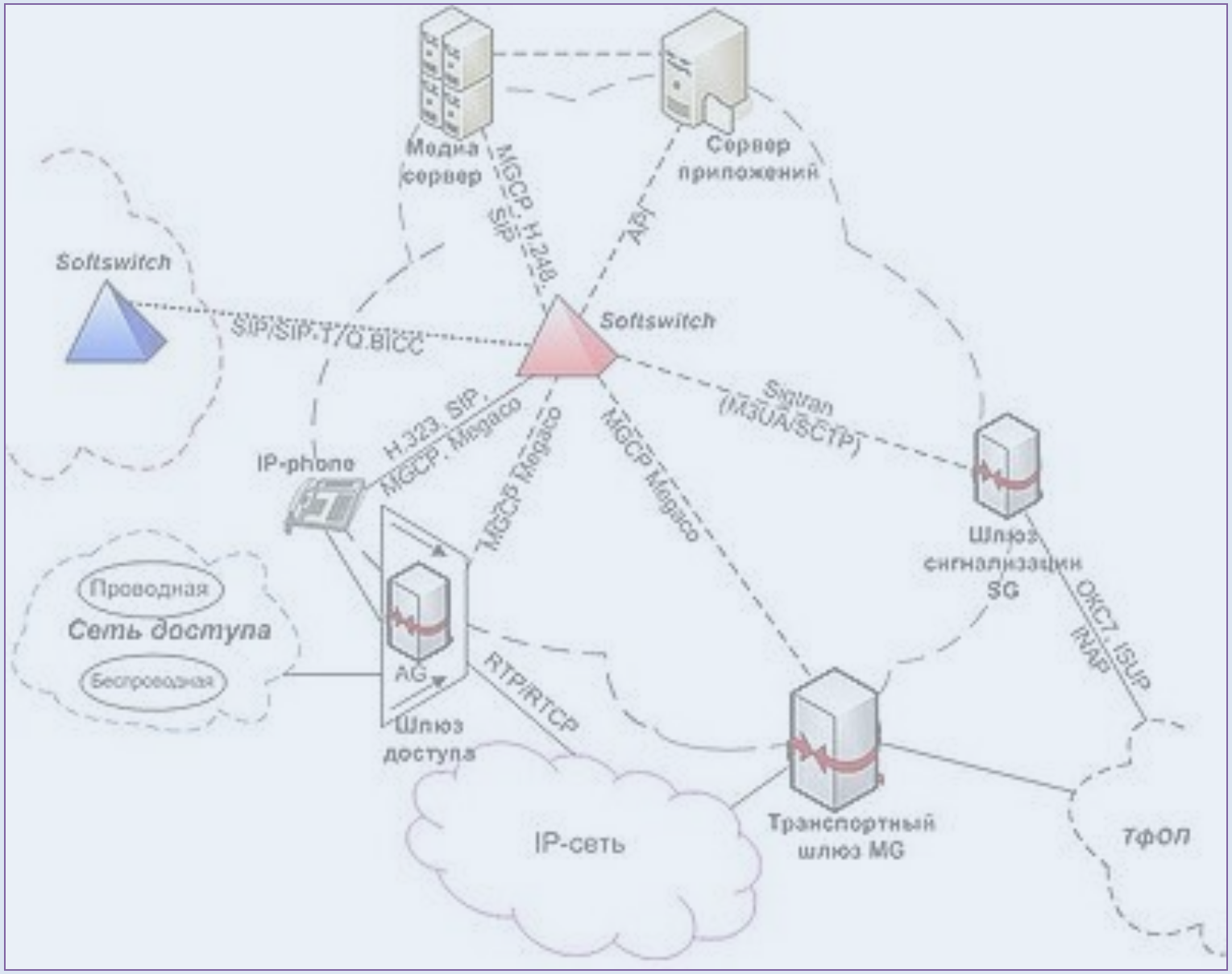
Абоненти ІКС

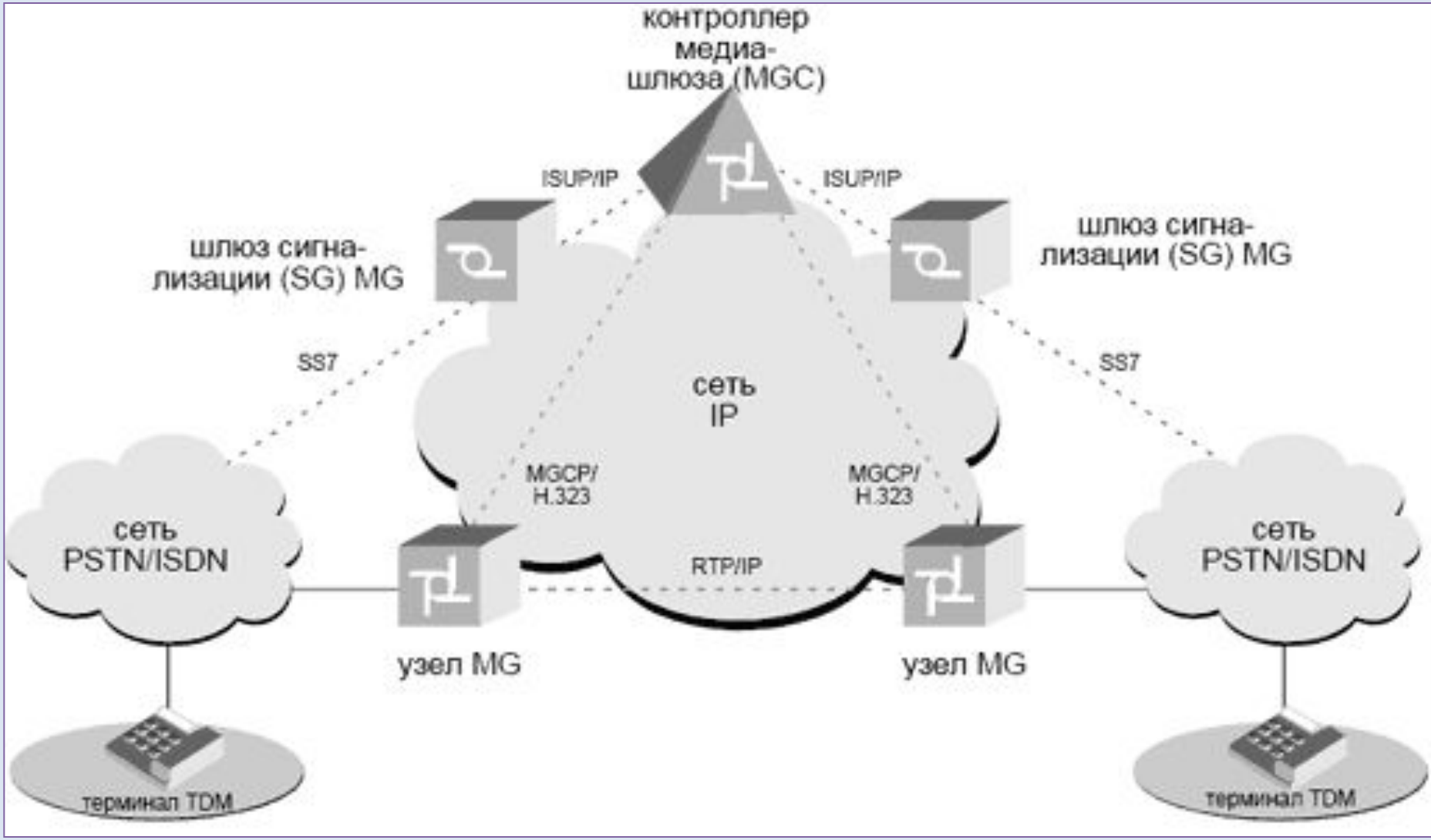
Рівень доступу та транспорту - перенесення інформації між кінцевими користувачами мережі NGN.

Як засоби доступу розглядаються практично всі використовувані в даний час варіанти, засновані на різних технологіях.

Порівння ТфОП та NGN




Медиа сервер
MGCP, H.248, SIP
Сервер приложений
API
Softswitch
SIP/SIP-T/Q.BICC
Softswitch
Signan (M3UA/SCTP)
H.323, SIP, MGCP, Megaco
IP-phone
MGCP Megaco
MGCP Megaco
Шлюз сигнализации SG
OKC7, ISUP, INAP
Проводная
Сеть доступа
Беспроводная
AG
Шлюз доступа
RTP/RTCP
IP-сеть
Транспортный шлюз MG
ТфОП


контроллер
медиа-
шлюза (MGC)
ISUP/IP
ISUP/IP
шлюз сигна-
лизации (SG) MG
шлюз сигна-
лизации (SG) MG
SS7
SS7
сеть
IP
MGCP/
H.323
MGCP/
H.323
сеть
PSTN/ISDN
RTP/IP
сеть
PSTN/ISDN
узел MG
узел MG
терминал TDM
терминал TDM

VOIP - Voice over IP - IP-телефония

система зв'язку, що забезпечує передачу мовного сигналу по IP-мережах.

Сигнал по каналу зв'язку передається в цифровому виді і може перед передачею перетворюватись (стискуватись) для видалення надлишковості.

- можливість передавати більш ніж один телефонний дзвінок
- конференція
- переадресація дзвінка
- автоматичне перенабирання
- визначення вхідного номера

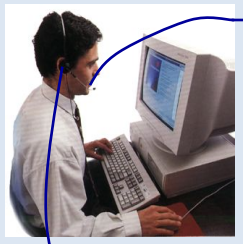
Переваги **VOIP**

- Безпечні дзвінки, із стандартизованим протоколом (SRTP). Оцифрування сигналу та його передавання вже вирішені в рамках технології VOIP. (Вибір шифрування сигналу, і його ідентифікацію для існуючого потоку даних окремо).
- Незалежність від місця розташування (лише доступ до Інтернет)
- Доступна інтеграція з іншими послугами (відео-дзвінок, обмін повідомленнями і даними під час розмови, аудіо конференції, управління адресною книгою, інформація про онлайн абонентів).
- Маршрутизація дзвінка, спливаючі вікна, альтернативний GSM-роумінг тощо. (телефонний дзвінок знаходиться в тій же самій мережі передачі даних, що і персональний комп'ютер користувача).
- Сумісність з мобільними технологіями

Процес зв'язку VoIP

1) Перетворення голосу
2) Встановлення зв'язку

Пакетне передавання голосу в сценарії «комп'ютер -комп'ютер» (без мережі ТфОП)



Мікрофон

АЦП

Компресія мовної інформації

Пакетизація

Керуванн сигнал

5. Connect 192.100.15.105

7. Ack open channel RTP

8. Голос в пакетах RTP

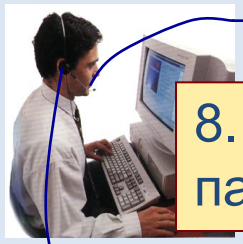
Наушники, динаміки

ЦАП

Декомпресія мовної інформації

Депакетизація

8. Голов в пакетах RTP



Мікрофон

АЦП

Компресія мовної інформації

Пакетизація

8. Голос в пакетах RTP

7. Ack open channel RTP

Наушники, динаміки

ЦАП

Декомпресія мовної інформації

Депакетизація

Кодування мовної інформації

При визові VoIP

1. Аналогово-цифрове перетворення
2. Стискання потоку (для зменшення необхідної смуги пропускання)
3. Розбиття оцифрованого голосу на IP-пакети (використовується протокол **RTP** (Real-time Transport Protocol)
4. Інкапсуляція пакетів RTP в пакети UDP, які і передаються по мережі

Протокол RTP використовує по два порти для кожного напрямку.

Один застосовується для передачі даних.

Інший для потоку RTPC (Real-time Control Protocol), який відповідає за якість послуг (Quality of Service, QoS) та керування.

Вокодер вносить додаткову затримку порядку 15-45 мс:

- використання буфера для накопичення сигналу і обліку статистики подальших відліків (алгоритмічна затримка);
- математичні перетворення, що виконуються над мовним сигналом, вимагають процесорного часу (обчислювальна затримка).

Основним джерелом виникнення спотворень, зниження якості і розбірливості синтезованої мови є переривання потоку мовних даних, викликане:

- втратами пакетів при передачі по мережі зв'язку;
- перевищенням допустимого часу доставки пакету з мовними даними.

Встановлення зв'язку

Процедура встановлення зв'язку залежить від конкретного протоколу

Протоколи VoIP

H.323 - сигналізація по портам (1720 TCP, 1719 TCP) для реєстрації терміналів на шлюзі.

SIP - забезпечує передачу голосу, відео, повідомлень систем миттєвого обміну повідомлень і довільного навантаження. Для сигналізації порт 5060 UDP. Підтримує контроль присутності.

IAX2 - через 4569 UDP-порт і сигналізація, і медіа-трафік (Asterisk Open Source VoIP).

MGCP (Media Gateway Control Protocol) протокол управління медіашлюзами.

Megaco/H.248 — протокол управління медіашлюзами, розвиток MGCP.

SIGTRAN — протокол тунелювання PSTN сигналізації SS7/ОКС7 через IP на SoftSwitch.

SCTP (Stream Control Transmission Protocol) — протокол для організації гарантованої доставки пакетів в IP-мережах.

SCCP (Skinny Call Control Protocol) — закритий протокол управління терміналами (IP-телефонами і медіашлюзами) в продуктах компанії Cisco.

Unistim — закритий протокол передачі сигнального трафіку в продуктах компанії Nortel.

Протоколи NGN

H.323
SIP
MGSP
MEGACO/H.248
SIGTRAN

Протокол H.323

H.323 – встановлення з'єднання і передачі голосового і відео трафіку по мережам IP, які не гарантують якості обслуговування (QoS).

Використовується протокол RTP, а також стандартні кодеки.

Протокол H.323 був першим в технології IP-телефонії.

Протокол SIP (Session Initiation)

Протокол прикладного рівня – операції з мультимедійними сесіями або викликами по IP-мережі:

- встановлення,
- зміна
- завершення.

В мультисервісних мережах SIP виконує функції, як і протокол H.323.

Сесії SIP можуть включати мультимедійні конференції, Інтернет-телефонію та інші додатки.

SIP де факто є міжнародним стандартом.

Протокол MGCP

Media Gateway Control Protocol - управління медіа шлюзами (MG).
Вся логіка обробки викликів розташовується поза шлюзами, і керування виконується зовнішніми пристроями, - MGC (Media Gateway Controller) або агентами викликів.
Модель викликів MGCP розглядає медіа-шлюзи як набір кінцевих точок, які можна з'єднати один з одним.

MEGACO/H.248

Заміняє MGCP для управління медіа-шлюзами.
MEGACO - платформа для шлюзів, пристроїв керування багатоточковими з'єднаннями та пристроїв інтерактивної голосової відповіді.
Підтримує різні системи сигналізації мереж з комутацією каналів, включаючи тонову сигналізацію, ISDN, ISUP, QSIG і GSM.
Кожне повідомлення є транспортним механізмом передачі команд

Протокол сигналізації транспорту (SIGTRAN)

Набір протоколів для передачі сигнальної інформації по IP-мережах.
Використовується MG, SG та Softswitch.
Реалізує функції протоколу SCTP і рівнів адаптації.

SCTP (Simple ControlTransport Protocol) відповідає за надійну передачу сигнальній інформації, здійснює управління сигнальним трафіком, забезпечує безпеку.

1) передача сигнальної інформації від відповідних сигнальних рівнів, що використовують послуги SCTP.

2) відповідальні за
- сегментацію і пакетування даних
- захист від імітації законного користувача,
- зміни сенсу переданої інформації
- тощо.

Загальні поняття

QoS (*Quality of service*) — якість обслуговування.
Імовірність того, що мережа зв'язку відповідає заданій угоді щодо трафіку (ймовірності того, що пакет пройде між двома точками мережі).

При передачі даних через IP-мережі (Інтернет) немає гарантій ні щодо затримки, ні взагалі з доставки, що неприйнятно для

-передачі голосу (пропускна здатність ≥ 16 кбіт/с, максимально допустима затримка <100мсек),
-відеоконференцій,
-додатків віртуальної реальності.

Основні параметри якості зв'язку

Bandwidth	Смуга пропускання	номінальна пропускна здатність середовища передачі інформації, визначає ширину каналу. bit/s (bps)
Delay	Затримка передачі пакета	мс
Jitter	Коливання (тремтіння)	затримки при передачі пакетів — джіттер, мс
Packet loss	Втрата пакетів	кількість пакетів, загублених у мережі під час передачі
	Вартість маршруту	найкоротший шлях
Errors	Помилки	Ймовірність спотворення одного біту інформації

Основні проблеми якості зв'язку

Низька пропускна здатність	У зв'язку з різним навантаженням від користувачів, максимальна пропускна здатність, яка надана певному потоку даних, може бути занадто низькою для мультимедійних послуг реального часу, якщо всі потоки даних отримують однаковий пріоритет
Затримка передачі пакета	Під час передавання пакет може потрапляти в довгі черги, або йти обхідним маршрутом, щоб уникнути заторів. Затримка може накопичуватися протягом довгого часу, навіть якщо пропускна здатність в межах норми, що може призвести до відмови в обслуговуванні
Коливання (Джиттер)	Пакети від джерела до кінцевого пункту надходять з різними затримками. Затримка пакета варіюється в залежності від його положення в чергах маршрутизаторів на шляху між джерелом і одержувачем, і може змінюватися непередбачувано. Джиттер може серйозно вплинути на якість передачі аудіо-відео.
Відкинуті пакети	Маршрутизатори можуть не доставити пакети, з пошкодженими даними або ті, що приходять, коли буфери повні. Приймач може вимагати повторної передачі, що викликає затримки
Помилки	Пакети пошкоджуються шумами і перешкодами. Приймач повинен виявляти такі помилки і може звернутися за цією інформацією повторно
Доставка поза чергою	При передаванні потоку, різні пакети можуть йти за різними маршрутами, і мати різні затримки. Отже пакети прибувають в іншому порядку, ніж при відправленні. Необхідні спеціальні додаткові протоколи для обробки пакетів за відповідною чергою. Це особливо важливо для відео та VoIP-потоків, де на якість значно впливають як затримки так і відсутність послідовності.

Jitter - Джиттер

Джиттер – випадкова затримка розповсюдження пакетів
Причини:
-Обмежена полоса пропускання або некоректна робота активних мережевих пристроїв
-Висока затримка розповсюдження сигналу
-Тепловий шум

Джиттер для i-го пакету:

$$J_i = J_{i-1} + (|D_{i-1}| - J_{i-1})/16$$

D_i – відхилення від очікуваного часу прибуття i-го пакету

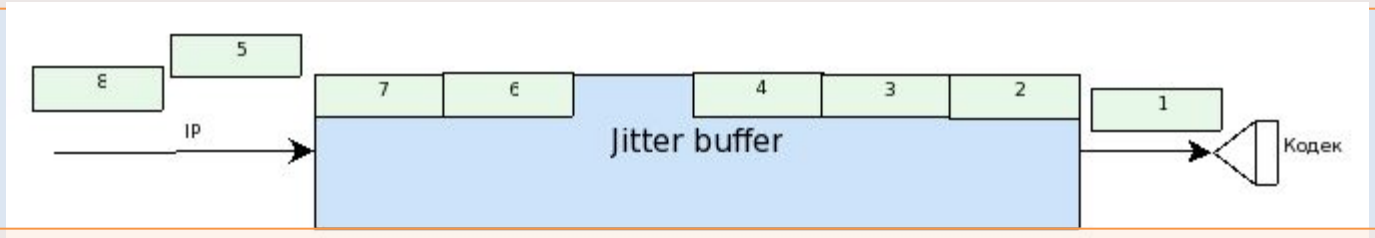
$$D_i = (R_i - R_{i-1}) - (S_i - S_{i-1})$$

R – час прибуття пакету у мітках часу RTT
S – часова мітка RTT взята з пакету

Джиттер у сучасних системах складає в середньому 5-10 мс.
При значеннях >100 мс, отримати звуковий сигнал майже не можливо

Jitter - Джиттер

Для компенсації нерівномірної швидкості отримання пакетів на приймальній стороні створюється тимчасове сховище пакетів – **джітер-буфер**.
Збирає пакети, що поступають, у порядку відповідному часовим міткам і надає їх кодеку з правильними інтервалами і в правильному порядку



Розмір буфера VoIP-приймач розраховує в процесі роботи (якщо не задано в налаштуваннях).
Буфер не повинен бути занадто великий, щоб не збільшувати транспортну затримку. Але маленький викликає втрати пакетів.
Протиріччя – З точки зору провайдера всі пакети доставлені абоненту, тобто втрат немає. З точки зору VoIP-пристрою, різниця між приходом пакетів перевищує джиттер-буфер. Тому фактично втрати є.
На практиці втрата більше ніж
1% - викликає неприємні враження
2% - розмова ускладнена
4% - розмова не можлива

Вимоги до якості обслуговування для голосу

У магістралях для VoIP-сервіса високої якості
-Втрати пакетів – > 0,25 %
-Одностороння затримка – >150 мс
-Джіттер – > 10 мс
-Гарантована пріоритетна полоса пропускання
-для розмови - 21- 106 кбіт/с
-для сигнального трафіку – 150 б/с

Вимоги до якості обслуговування для відео

Для відеоконференцій
-Втрати пакетів – > 1 %
-Одностороння затримка – >150 мс
-Джіттер – > 30 мс
-Гарантована пріоритетна полоса пропускання
-розмір відео-сесії +20 %

Для потокового відео
-Втрати пакетів – > 2 %
-Одностороння затримка – > 4-5 с
-Джіттер – > відсутні вимоги (буферизація на рівні застосунку)
-Гарантована пріоритетна полоса пропускання
- пропускна здатність каналу

З чого все починалось

Для приймання і відправлення пакетів на маршрутизаторах у найпростішому випадку застосовують метод FIFO: перший прийшов — перший пішов (First In — First Out)

У випадку перевантаження мережі – на маршрутизаторах утворюються затори, які розв’язують так:
Усі пакети, що не ввійшли до буферу черги FIFO (як на вході, так і на виході), ігноруються маршрутизатором, тобто просто втрачаються

Більш досконалий метод — застосовувати «розумну» чергу, в якій пріоритет пакетів залежить від типу сервісу — ToS
Для створення «розумної» черги пакети повинні заздалегідь отримати мітки типу сервісу

IP-заголовок TOS (Type of service)

1981 р. перші спроби введення параметрів якості обслуговування.
RFC-791 – IP-заголовок TOS (Type of service) 1992 р. RFC-1349

0	1	2	3	4	5	6	7
Пріоритет							
Мінімальна затримка			1	0	0	0	0
Максимальна пропускна здатність			0	1	0	0	0
Максимальна надійність			0	0	1	0	0
Мінімальна вартість			0	0	0	1	0
Загальні послуги			0	0	0	0	0

Протоколи, що надають послугу QoS

Поле ToS у заголовку IPv4
IP Differentiated services (DiffServ)
IP Integrated services (IntServ)
Resource reSerVation Protocol (RSVP)
Multiprotocol Label Switching (MPLS)
RSVP-TE (Traffic Engineering)
Frame relay
X.25
Asynchronous Transfer Mode (ATM)
IEEE 802.1p/Q
IEEE 802.11e
IEEE 802.11p

Моделі QoS

Best Effort Service	Integrated Service (IntServ)	Differentiated Service (DiffServ)
Негарантована доставка	Інтегроване обслуговування	Диференційоване обслуговування
просте збільшення пропускної здатності без виділення окремих класів трафіку та регулювання	забезпечує наскрізну якість обслуговування, гарантуючи необхідну пропускну здатність	керування формуванням трафіку (класифікація пакетів, маркування, керування інтенсивністю) і керування політикою (розподіл ресурсів, політика відкидання пакетів).

Integrated Service (IntServ) – Інтегроване обслуговування

Згідно RFC 1633, модель IntServ забезпечує наскрізну (End-to-End) якість обслуговування, гарантуючи необхідну пропускну здатність

IntServ використовує протокол резервування мережевих ресурсів **RSVP**, що забезпечує виконання вимог до всіх транзитних вузлів
Тому також використовується термін «резервування ресурсів» (**Resource reservation**)

IntServ (L3) = ATM (L2)

4 класи QoS

QoS Class 1	клас послуг A	має ті ж характеристики, що й виділений цифровий канал точка-точка
QoS Class 2	клас послуг B	забезпечує режим, прийнятний для аудіо та відео при відеоконференціях або передачі мультимедіа
QoS Class 3	клас послуг 3	забезпечує режим, прийнятний для передачі, орієнтованої на з'єднання, наприклад, через Frame Relay
QoS Class 4	клас послуг 4	еквівалентний режиму IP-передачі в умовах найкращих зусиль (best efforts) при відсутності гарантії доставки.

IntServ – Протокол RSVP (Internet Resource Reservation Protocol)

Надає сигнальний механізм для конфігурування віддалених маршрутизаторів з метою отримання потрібного QoS.

Орієнтація на одержувача: дозволити одержувачу керувати процесом
- масштабованість (scalability)
- гетерогенність (heterogeneity)

Гнучкий стан: стан виклику (резервування) у маршрутизаторах не повинен чітко видалятися
- буде усунено, якщо не “оновиться” одержувачами

Три види трафіку

Характеристика	Best Efforts	Rate-sensitive Чутливий доазавантаження	Delay-sensitive Чутливий до затримки
	передача IP-даних без встановлення з'єднання	клас послуг з гарантованою швидкістю в бітах у секунду	передача голосу або відео
Пропускна здатність	впливає	Канал з гарантованою пропускною здатністю	Може змінюватись
Затримки	впливає	викликає	Мінімальна затримка
Джіттер	Не впливає	Не впливає	Мінімальний джіттер

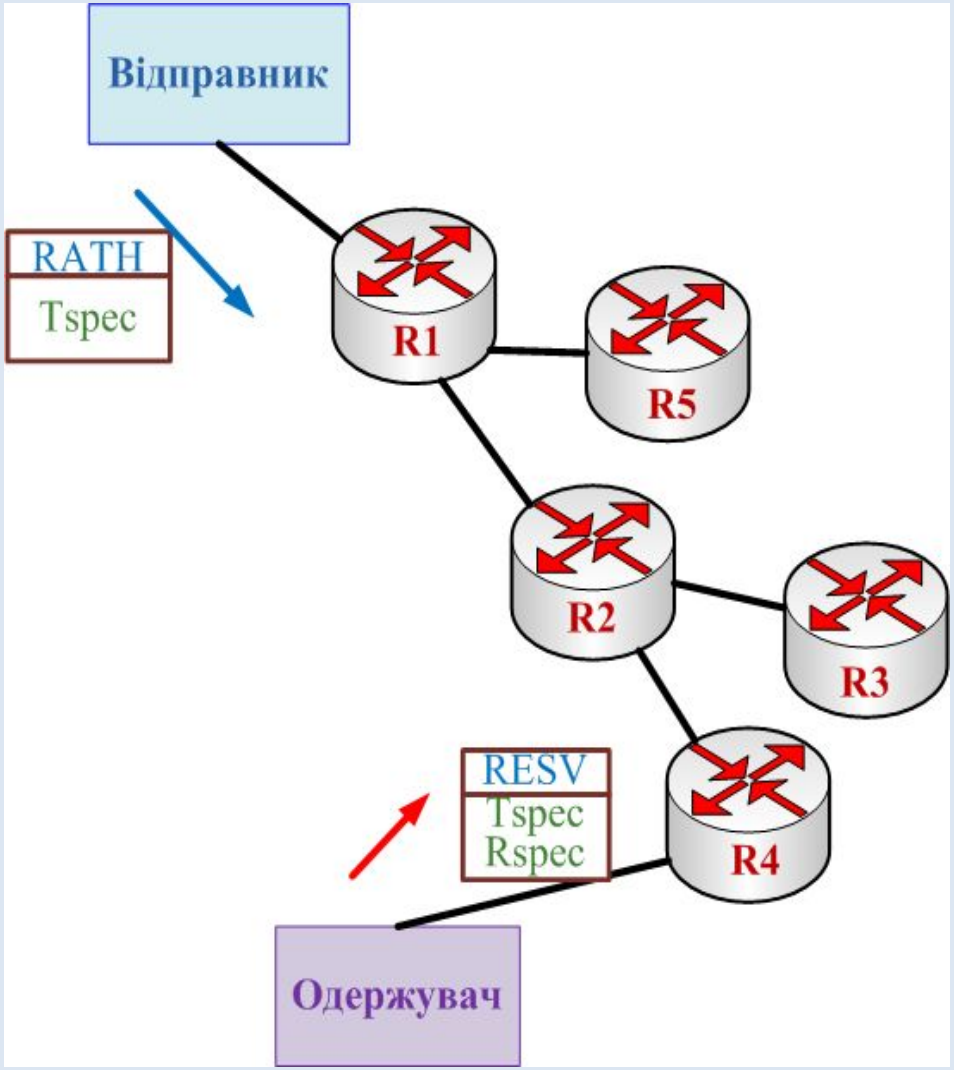
IntServ –
RSVP: Протокол встановлення виклику

Відправник надсилає Tspec до групового дерева у повідомленні PATH

Одержувач надсилає назад повідомлення RESV у зворотному напрямку

- містить Tcpec відправника та вимоги до QoS одержувача (Rspec)

Маршрутизатори, які знаходяться на зворотному шляху виділяють ресурси необхідні для задоволення вимог QoS одержувача



IntServ –
RSVP: Протокол встановлення виклику

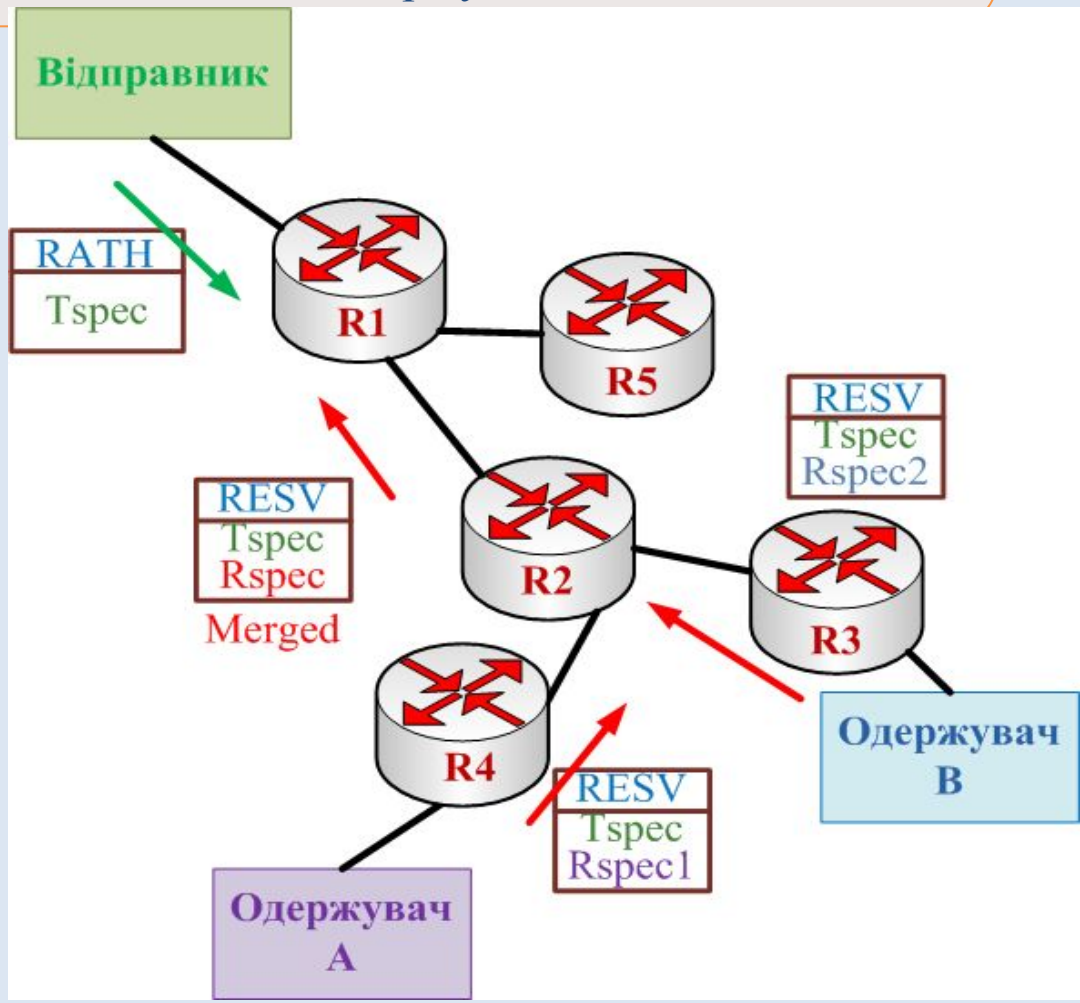
Велика кількість одержувачів:

- можуть мати різні вимоги QoS
- резервування ресурсів об'єднується як тільки RESV передається відправнику
- ресурси потрібно резервувати для задоволення вимог одержувачів

Одержувач А спершу резервує ресурси для максимальної затримки 100 мс

Якщо Одержувач В вимагає для QoS максимальну затримку у 200 мс нові ресурси на R2, R1 не виділяються

Якщо Одержувач В вимагає для QoS максимальну затримку 50 мс, для R2, R1 слід виділити додаткові ресурси



Черга WFQ 8 рівнів пріоритету

Пріоритет керування мережею (7)
Пріоритет управління Інтернет = межмережеве керування (6)
Критичний пріоритет (5)
Екстрений пріоритет (4)
Негайний пріоритет (2)
Переважний пріоритет (1)
Ордінарний пріоритет (0)

Differentiated Service (DiffServ)
Диференційоване обслуговування

Описане в RFC 2474 и RFC 2475

Забезпечує QoS на основі розподілу ресурсів всередині мережі та певних класифікаторів і обмежень на межі мережі

Розділення трафіку по класах, для кожного з яких визначають свій рівень QoS

DiffServ

керування формуванням трафіку

- класифікація пакетів
- маркування
- керування інтенсивністю

керування політикою

- розподіл ресурсів
- політика відкидання пакетів

DiffServ
Механізми керування трафіком

Формування трафіку (traffic shaping, rate limiting)

Leaky bucket

відро, що протікає

Token bucket

іноді помилково ототожнюють з алгоритмом leaky bucket

TCP rate control

(керування швидкістю TCP) — штучне регулювання розміру вікна TCP разом з керуванням темпу повернення квитанцій ACK відправнику

Алгоритми планування (Scheduling algorithms)

Weighted fair queuing (WFQ)

справедлива черга з ваговими коефіцієнтами

Class based weighted fair queuing

справедлива черга з ваговими коефіцієнтами на підставі класів

Weighted round robin (WRR)

перебирання по колу з ваговими коефіцієнтами

Deficit weighted round robin (DWRR)

Hierarchical Fair Service Curve (HFSC)

Запобігання перевантаженню (Congestion avoidance)

Random early detection (RED, WRED)

алгоритм активного керування чергами, що зменшує ймовірність відкидання пакетів з кінця черги у буфері

Policing

маркування/відкидання пакетів, що не відповідають вимогам угоди щодо інтенсивності трафіку і обсягу сплесків

Explicit congestion notification

явне повідомлення про перевантаженість (TCP)

Buffer tuning

налаштування буферів

Алгоритм Leaky Bucket (meter)

Відро, що протікає, як вимірювач

З кожним користувачем, що передає пакети, асоціюють лічильник

Користувач встановлює темп зменшення лічильника (задає середню перепускну здатність) і межу (міру сплесків)

-Лічильник збільшують, коли користувач надсилає пакет,

якщо лічильник перебільшує встановлену межу, пакет вважають таким, що не відповідає вимогам (non-conformant)

- Лічильник зменшують періодично (через рівні проміжки часу),

Алгоритм Leaky Bucket (queue)

Відро, що протікає, як черга

Існує черга заданої довжини

Коли надходить пакет, якщо у черзі є достатнє місце для нього, його додають у чергу, якщо ж немає – його відкидають

Через рівні проміжки часу один пакет відправляють у мережу (якщо черга не порожня)

Таким чином, “відро” формує рівномірний трафік

Алгоритм Token Bucket

Відро маркерів

Через рівні проміжки часу у відро кладуть один маркер

Відро може утримувати певну кількість маркерів. Якщо маркер надходить коли відро повне, його ігнорують

Коли надходить пакет розміром в n байт, n маркерів забирають з відра, а пакет надсилають у мережу

Якщо у відрі менше, ніж n маркерів, з відра нічого не забирають, а пакет вважають таким, що не відповідає вимогам (non-conformant)

Алгоритм *Token Bucket* еквівалентний алгоритму *Leaky Bucket as a meter*

ці два алгоритми є дзеркальним відображенням один одного, але вони дають тотожні результати щодо визначення відповідності трафіку

Безпека NGN

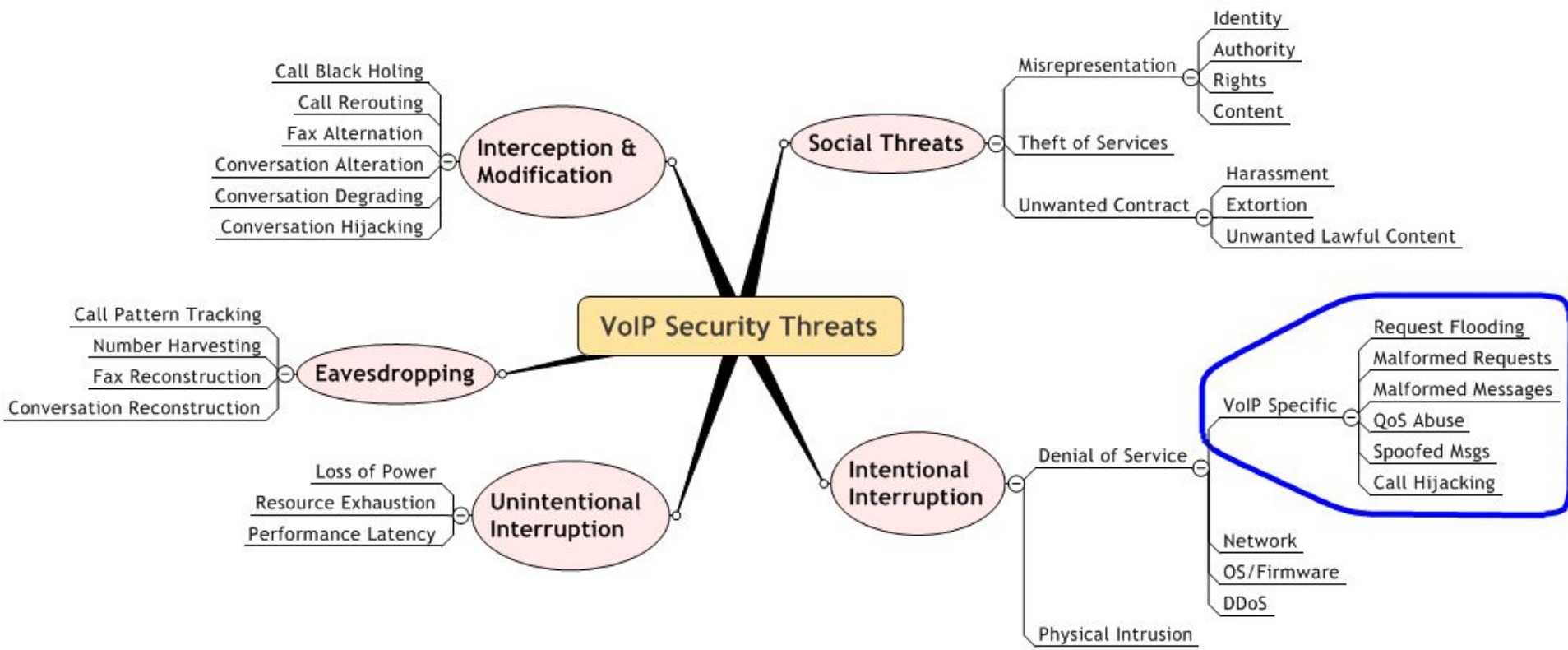
Безпека як послуга входить до складу послуг контролю мережі:

- ✔*надійності,*
- ✔*сталості,*
- ✔*підзвітності,*
- ✔*спостережності,*
- ✔*експлуатаційних властивостей,*
- ✔*адміністрування клієнта,*
- ✔*навантаження (трафік),*
- ✔*керування маршрутизацією.*

Особливості безпеки VoIP

—відсутність шифрування, відповідно - прослухування VoIP-дзвінків, і навіть зміна їх вмісту
—Аналізатори мережевих пакетів перехоплює пакети
—Велика чутливість до DoS-атак
—Можливість створювати та підробляти пакети SIP (SiVus)
—Відкриті кодеки легко декодуються
—атаки на мережі IP використані для атак на VoIP

- Підготовка та атестація IP-телефонів
- Спуфінг Caller ID (підробка ідентифікатора абонента)
- Крадіжка обслуговування VoIP
- Викрадення облікового запису в SIP
- Маскування під SIP-проксі
- Фальсифікація повідомлень SIP та RTP / ін'єкції
- Перетворення сигналів SIP в SS7
- Проблеми з NAT
- Фрод на основі голосової пошти
- Взаємодія з правоохоронними органами



- відсутність шифрування, відповідно - прослухування VoIP-дзвінків, і навіть зміна їх вмісту
- Аналізатори мережевих пакетів перехоплює пакети
- Велика чутливість до DoS-атак
- Можливість створювати та підробляти пакети SIP (SiVus)
- Відкриті кодеки легко декодуються
- атаки на мережі IP використані для атак на VoIP

Фрод

Згідно Рекомендації МСЕ-Т Е.408, однією з характеристик ризику ІБ в мережах зв'язку є наслідок реалізації загроз.
Шахрайство у мережах зв'язку називають Фродом - Нечесна спроба переконати сторону в легітимності транзакції тоді, як насправді цього немає.

Мета:

- фінансова
- плагіат
- шахрайство в процесі виборів,
- лжесвідчення.

Асоціація по контролю над фродом у ТКС - Communications Fraud Control Association, CFCA

Subscription Fraud - Шахрайство з підпискою

Шахрай підписується на послугу легальним способом (як правило, не від свого імені).
При цьому він може:
а) використовує сервіс в особистих цілях з метою мінімізувати свої витрати або зовсім не платити;
б) виконує дії, спрямовані на отримання прибутку, - перепродує послуги.

У мережах NGN приділяється велика увага захисту за допомогою механізмів автентифікації від шахрайства з підпискою

Identity Take Over - Перехоплення або крадіжка підписки

шахрай отримує можливість використовувати послуги від імені легітимного користувача.
Наприклад, компрометація облікового запису абонента, після чого зловмисник починає активне використання послуг за рахунок власника скомпрометованого акаунта

Bypass Fraud - Шахрайський обхід

Вибір неавторизованих маршрутів проходження сигналізації та|або трафіку.

Оператори зв'язку, прагнучи скоротити свої витрати міжнародного (міжміського) трафіку через мережі транзитних операторів, використовують технологію VoIP для незаконної організації прямих IP-каналів до операторів-одержувачів цього трафіку, в обхід зонових, міжміських чи міжнародних транзитних вузлів зв'язку.

Інша форма шахрайства, основана на тому, що мережа SIP допускає встановлення сесій безпосередньо між кінцевими терміналами без участі SIP-проксі оператора.

Такі виклики не фіксуються оператором, так як SIP-проксі (першоджерело для отримання тарифікаційних даних) оператора не бере участь у сигнальному обміні.

Шахрай може організувати пропуск трафіку по мережі оператора зв'язку в своїх цілях. Виявити дозволяє аналіз даних з різних мережних пристроїв, що виявляє аномалії в проходженні трафіку.

Маніпуляція сигнальних повідомлень (Manipulation SS7)

спотворення адреси абонента в повідомленні IAM (ТфОП / ISDN) або UDT (мережі GSM) системи сигналізації ОКС № 7.
У мережі сигналізації SIP дана форма фроду може бути реалізована маніпуляцією полів From та Contact в сигнальних повідомленнях.
В результаті реалізації фроду система тарифікації викликів не зможе правильно тарифікувати з'єднання

Private Branch Exchange, PBX або Voice Mail

Шахрайство, засноване на вразливості в АТС або голосовій пошті.
Наприклад, системи голосової пошти можуть бути сконфігуровані так, що будуть ініціювати виклик автору повідомлення після того, як користувач прослухав голосове повідомлення.
Шахрай може скористатися цим функціоналом, отримавши доступ до голосової поштової скриньки.
отримання зловмисником доступу до SIP-проксі серверу оператора або до станцій корпоративних користувачів АТС

Шахрайство, засноване на уразливості при реалізації додаткових видів обслуговування (ДВО)

ДВО надають широкі можливості абонентам, серед яких переадресація виклику, очікування виклику, перенаправлення виклику, участь у конференції, обмеження вхідного і (або) вихідного зв'язку

Абонент, який має доступ до ДВО, активує відповідну послугу зі свого термінала за допомогою спеціального сервісного коду.

Шахрай активує послугу переадресації абоненту-жертві, послявши від її імені скомпрометований сервісний код.

В результаті виклики, що надходять на номер абонента-жертви, будуть переадресовуватися на необхідний шахраєві номер. Оплата за переадресовані виклики буде нарахована на рахунок абонента-жертви.

Domestic Revenue Share Fraud, DRSF

Фрод розподілу доходу між операторами країни
Ця форма фроду підлягає контролю CFCA і передбачає зловмисні дії недобросовісного оператора, спрямовані на отримання незаконного прибутку при взаємодії з суміжними операторами тієї ж країни.
Генерація фіктивного великого обсягу трафіку від мережі оператора-жертви на мережу оператора-шахрая.

International Revenue Share Fraud, IRSF

Фрод розподілу доходу між операторами різних країн
Аналогічний DRSF, але передбачає зловмисні дії недобросовісного оператора щодо іноземного оператора-жертви.

Premium Rate Service - Фрод при використанні служб привілейованого тарифу

- платні служби, послуги розважального чи інформаційного характеру. Здійснюючи виклик на номери служб привілейованого тарифу, абонент оплачує як послуги оператора зв'язку (за організацію з'єднання), так і інформаційну послугу, що надається постачальником інформації.
- ініціація **шахраєм** від скомпрометованого акаунта легітимного абонента великого числа викликів на службу привілейованого тарифу, власником якої є шахрай, оплата абонентами-жертвами послуг, що надаються іншим абонентам.
- послугу нелегітимно запитує сам **оператор.** При цьому оплата за надання послуги переводиться з рахунку постачальника-жертви інформації на рахунок оператора мережі зв'язку.

Clonning Клонування

Шахрай створює копії в цілях отримання безкоштовних послуг мережі зв'язку.
Прикладом в мережі GSM може бути клонування SIM-карт мобільної станції.

Використання технічним персоналом доступною йому службової інформації з метою вчинення шахрайства

Співробітники телекомунікаційних компаній тим чи іншим способом співпричетні в 73% випадків шахрайства.
(Згідно з даними звіту CFCA за 2011 р.)

Фрод при використанні кредитної картки

Для отримання послуг в мережі IP-телефонії може бути використання шахраєм вкраденою кредитної картки

Результати

- У наведений вище список включені форми фроду, які завдають найбільшої шкоди (за даними CFCA за 2011 р.).
- Так, шахрайство з підпискою становить 10,8%, а IRSF - 9,8% від частки нанесення збитку іншими формами фроду.
- Згідно з цим же звітом CFCA , втрати в індустрії зв'язку в 2011 р. склали 40,1 млрд дол, що відповідає 1,88% від загального прибутку галузі.
- У деяких джерелах реальні сумарні втрати нових операторів зв'язку в результаті шахрайства складають до 20% від їх сумарного доходу

Аспекти безпеки NGN

- Автентифікація
- Авторизація
- Реєстрація дій користувачів

- Мобільні агенти
- З'єднання
- Домашніх мереж

Вимоги безпеки (X.805)

- Контроль доступу
- Автентифікація
- Неможливість відмови від виконаних дій
- Конфіденційність
- Цілісність
- Доступність
- Конфіденційність трафіку
- Забезпечення приватності

Вимоги безпеки NGN (рекомендації ITU)

- розподіл ключів як для кінцевих користувачів, так і для елементів мережі;
- автентифікація та авторизація для різних видів доступу, а також різного QoS;
- стандартизація проходження трафіку VoIP через міжмережеві екрани
- надійна автентифікація та контроль над суб'єктами інформаційного обміну
- запобігання спаму (в тому числі в голосових повідомленнях)
- конвергенція безпеки зв'язку з IT-безпекою

Захист VoIP

- Використання шифрування VoIP-трафіку (SSL/TLS)
- Використання строгої автентифікації
- Використання Voice VPN (яке є поєднанням технології VOIP і VPN) надає можливість створення безпечного голосового з'єднання для VoIP-мереж усередині компанії, шляхом використання IPSec.
- Та інших методів захисту мереж

Безпека VoIP – Мінімальна оборона

Використання автенифікації (метод запит-відповідь) на основі гешування SIP

1. Сервер надсилає клієнту певне значення (випадкове число, поточний час тощо), який клієнт гешує (MD5) на основі спільного секрету
2. Геш відсилається до сервера для перевірки та автентифікації

При цьому

- пароль не передається мережею
- запобігається атака повторного пересилання повідомлення
- забезпечується цілісність повідомлення

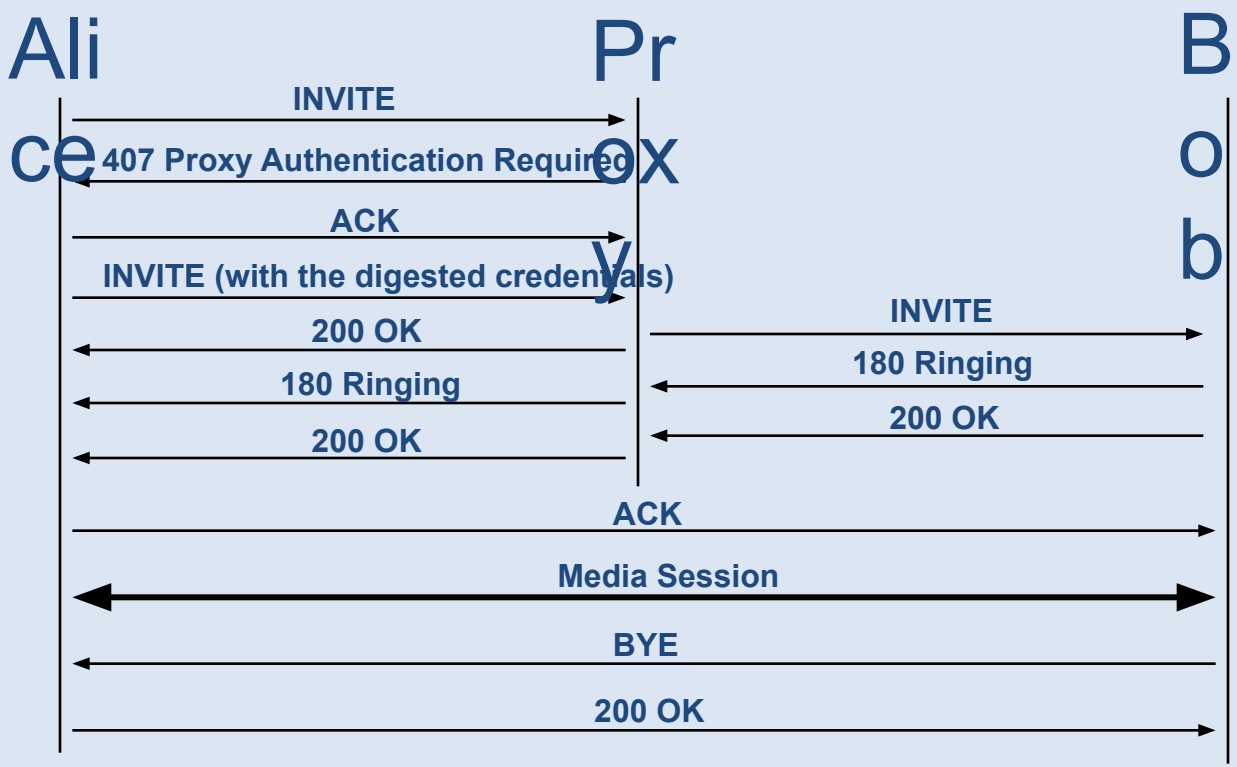
- Безпека буде слабкою, якщо випадкова послідовність зберігається більше ніж за один період

Покращити безпеку можна з використанням:

- Підрахунку кількості успішних з'єднань.
- Наступного випадкового числа, який сервер надсилає клієнту при наступному запиті (значно збільшує трафік при тунельному з'єднанні)

Безпека VoIP – Мінімальна оборона

SIP Digest Authentication



Безпека VoIP – Мінімальна оборона

- Шифрування при ініціалізації IP-телефонії
- Використання апаратного софтсвіча (зазвичай багатосервісно)
- Використання меж ціна/сесія в середині комутатора додатків
- Використання IPSec при SIP-з'єднаннях
- Захист DNS (досить важко)
- Використання сканерів вразливостей
- Не довіряйте мережі керування
- Визначення специфічних даних у процес аналізу шахрайств

Покращена безпека VoIP – SBC - Session Border Controller - прикордонний контролер сесій

- Використання контролера меж сесії
- Альтернативна маршрутизація на рівні SIP та RTP
- SIP-проксі для вхідних та вихідних повідомлень
- Контроль допустимості викликів
- Керування міжмережевим екраном RTP
- Переписування рівня SIP для проходження NAT
- Переписування рівня SIP для приховування топології
- Збирання даних про стан SIP-виклику для оптимізації ресурсів softswitch
- Збирання даних для допомоги правоохоронним органам

VoIP – SBC Session Border Controller — прикордонний контролер сесій

ALF = Application Layer Firewall

У VoIP ALF – це система запобігання вторгнень у SIP

Industry Challenges:

- Service Providers:
  - Collaborate on accumulating security related actuarial information
- Standards Bodies:
  - ANSI/ITU developed architectural security framework
  - Technology standards groups follow ANSI/ITU framework and leverage existing standard technologies (IPsec, PKI)
  - Accommodate today's reality (NAT, Firewalls, untrusted networks)
- Vendor Community:
  - Consider current best practices (e.g.. RFCs 2196, 2504, 3365)
  - Build on standards (IPsec, PKI, NIST Common Criteria, ATIS, ITU-T, ISO)
  - Support future needs (IPsec, IPv4 to IPv6 migration, PKI)
  - Adjust product plans to today's security realities (NAT is a fact and everywhere, NO network segments can be assumed trustable)

Механізми захисту протоколу SIP

1. Автентифікація за допомогою дайджеста повідомлення RFC 2617. Використовується алгоритм MD5 для отримання хеш-значення від імені, паролю та URL. Для конфіденційності медіа-даних використовують протокол SRTP (Secure Real-time Transport Protocol), а для обміну ключами використовують протокол SDP (Session Description Protocol) RFC 2327.
2. Забезпечення криптографічної безпеки електронної пошти на основі стандарту S/MIME (Secure/Multipurpose Internet Mail Extensions).
3. Використання протоколу TLS як для автентифікації, так і для шифрування даних.
4. Використання протоколу IPSec, що дозволяє здійснювати підтвердження достовірності і шифрування IP-пакетів та розподілення ключів за допомогою протоколу IKE (Internet Key Exchange).
5. Використання протоколу IPSec та ручне розподілення ключів.

Безпека Skype

Закритий протокол, тому не бажаний з т.з. безпеки

використовує TCP та UDP-протоколи для установлення сесій.

Автентифікація через Інтернет (навіть якщо користувачі знаходяться в одній мережі). Можливо створити вузол, який зможе виконувати, крім стандартних, ще й додаткові функції

- перенаправляти запити користувачів на підконтрольний сервер та блокувати деяким користувачам доступ до системи (атака на відмову в обслуговуванні);
- перехоплювати логіни та паролі користувачів;
- записати всю розмову або деяку її частину

Реалізація атаки “людина посередині”

Використовуються RSA-ключі та шифрування, подібне AES, але офіційних даних щодо алгоритмів шифрування розробник не надає

Передавання голосу по VPN

Вимоги

Втрата пакетів – не більше 1%

Затримка – не більше 150 мс

Варіація затримки – 30 мс

Розподіл потоків даних за пріорітетами

Приклади порушення безпеки

Хакери взламують VoIP-системи невеликих банківських відділень і від їх імені дзвонять клієнтам банку, вимагаючи назвати дані кредитних карт.

Взламування VoIP-системи провайдерів шляхом грубого перебору паролів обладнання та подальше використання послуг безкоштовно

UCSniff – набір утиліт для взламування VoIP

Аналіз локальної мережі і знаходження VoIP-мережі

Перенаправлення голосового трафіку

Автоматично записує дзвінки

Приховування інформації в VoIP-потоці використовуючи наприклад

- невикористовувані поля в протоколах RTCP (Real-Time Control Protocol) и RTP (Real-Time Transport Protocol)
- Затримку аудіо-пакетів

Програма SIPtap відслідковує трафік VoIP і записує його в форматі WAV для подальшого дослідження. Проникає в систему-жертву через троянську програму