ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ



ФАКУЛТЕТ ПО ТЕЛЕКОМУНИКАЦИИ

КАТЕДРА „КОМУНИКАЦИОННИ МРЕЖИ“

# КУРСОВ ПРОЕКТ

по

**Мултимедийни технологии и приложения (МТП)**

Студент: НИКОЛАЙ СТАНИМИРОВ ПРОДАНОВ

Група: 232 Фак. №: 111321045 E-mail: nikiavatar98@abv.bg

|  |
| --- |
| **23** |

**IMS услуги. Услуги, базирани на CAMEL. Взаимодействие между CAMEL базирана логика на услуги и SIP мениджмънт на сесии. Основни модели за управление на повиквания. Управление на GPRS сесии за данни. Управление на SMS. Управление на IP мултимедийни повиквания**

**Изходни данни:**

1. Мрежова технология и архитектура: IP-based Multimedia Subsystem (IMS)
2. Сигнализация: Session Initiation Protocol (SIP)
3. Описание на медийни сесии: Session Description Protocol (SDP)
4. Методи за информационна сигурност: IPSec/TLS
5. Автентикация/Оторизация/Таксуване: Diameter
6. IMS услуги: глас, видео, данни

Ръководител: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(доц. Кирил Късев)

МТП – магистър | Задание за Курсов проект (2021)

**Обща информация:**

Курсовият проект (КП) трябва да бъде в обем не по-малък от 25 А4 страници и да е разработен на български език, с изключение на специфични термини, за които няма общоприет превод. Препоръчителен шрифт Times New Roman, 12 pt или 14 pt, междуредие 1.5, двустранно подравнен текст. Страниците трябва да се номерират.

Всеки курсов проект се защитава спрямо предварително уточнен график (през последна учебна седмица или по време на редовна и зимна поправителна сесия).

Проектът се оценява. Тази оценка е самостоятелна и не зависи от това как студентът се е представил на изпита по дисциплината.

Структура на проекта:

* Заглавна страница с темата на курсовия проект и името на студента
* Теоретична част: въведение в тематиката и състояние на проблема според налични литературни източници. Обемът й не трябва да е повече от 40 % от пълния обем на проекта
* Решение на поставената задача: самостоятелно решение (анализи, сравнения, проектиране, изследване) на поставения в заданието проблем или задача
* Изводи и заключение - с обем не по-малък от 1/2 печатна страница
* Списък с използваните съкращения
* Списък с използваните литературни източници

Литература:

1. Alan B. Johnston, SIP: Understanding the Session Initiation Protocol, Artech House, 2015.
2. Rogero Perea, Internet Multimedia Communications Using SIP, A modern Approach Including Java Practice, Morgan Kaufmann publishers, Elsevier 2008.
3. \* Miika Poikselka, Georg Mayer, The IMS: IP Multimedia Concepts and Services – Third Edition, Weley, 2016.
4. \* Hu Hanrahan, Network Convergence, Services, Applications, Transport and Operation Support, Wiley, 2007.
5. Интернет източници

\* Източникът до голяма степен покрива темата на КП

|  |  |
| --- | --- |
|  | ОЦЕНКА – КП: |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| (дата на предаване) | (Ръководител „КП“) |

МТП – магистър | Задание за Курсов проект (2021)

Съдържание

[КУРСОВ ПРОЕКТ 1](#_Toc95776678)

[Част 1: Session Initiation Protocol (SIP): 4](#_Toc95776679)

[1. Основни характеристики на SIP 4](#_Toc95776680)

[2. Структура на SIP съобщение 5](#_Toc95776681)

[3. Видове SIP агенти 5](#_Toc95776682)

[4. Пример 5](#_Toc95776683)

[Част 2: Архитектура на IP-based Multimedia Subsystem (IMS) 6](#_Toc95776684)

[Част 3: CAMEL 7](#_Toc95776685)

[Част 4: Session Description Protocol (SDP) 8](#_Toc95776686)

[Част 5: Методи за информационна сигурност: IPSec/TLS 9](#_Toc95776687)

[1. Transport Security Layer (TLS) 9](#_Toc95776688)

[2. Internet Protocol Security (IPSec) 9](#_Toc95776689)

[Част 6: IMS услуги глас, видео, данни 10](#_Toc95776690)

[1. IMS услуги 10](#_Toc95776691)

[2. Услуги, базирани на CAMEL 10](#_Toc95776692)

[3. IM-SSF 10](#_Toc95776693)

[4. Управление на GPRS сесии за данни 10](#_Toc95776694)

[5. Управление на SMS 10](#_Toc95776695)

[6. Управление на IP мултимедийни повиквания 10](#_Toc95776696)

[Част 7: Изводи 11](#_Toc95776697)

# Session Initiation Protocol (SIP):

## Основни характеристики на SIP

Session Initiation Protocol (SIP) е протокол предоставящ възможности за сигнализация и контрол върху при изграждане, поддържане и разпадане на сесии. SIP протоколът може да управлява сесии от всякакъв вид но се използва основно за управление на аудио, видео и чат сесии, както и за интерактивни игри и виртуална реалност. Използва се за предоставяне на Voice Over Internet Protocol (VoIP) услуги, за Instant Messaging (IM) в Next Generation Networks (NGNs), както и за изграждане на бъдещи приложения и услуги.

SIP протоколът е разработен основно от SIPCORE работната група, която е част от Internet Engineering Task Force (IETF) и представлява алтернатива на предложението на IT-U H.323, но за разлика от H.323, SIP е по-лек (не се нуждае от значителни ресурси), текстово-базиран протокол с общо предназначение.

SIP е базиран на HyperText Transfer Protocol (HTTP), като от него наследява формата и подредбата на съобщенията си, както и Simple Mail Transfer Protocol (SMTP) от който наследява подхода за резолюция (откриване на IP адреса) на имената на потребители.

SIP е независим от протоколът на транспортният слой при което SIP съобщенията може да се пренасят от почти всички транспортни протоколи като Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Stream Control Transmission Protocol (SCTP) както и (ТLS) (въпреки че TLS не е точно транспортен протокол).

За изграждане на самата сесия предимно се използва Real-time Transport Protocol (RTP) или Secure Real-time Transport Protocol (SRTP). Тези протоколи практически създават каналът за данни по които ще се предава информация аудио, видео и д.р. При изграждането на тези канали за данни трябва да се зададат точни параметри за качество, функционалности които ще се използват, защитни параметри и всякакъв вид настройки необходими за сесията. Една от ролите на SIP е да предостави на двете (или повече) стани които искат да изградят канал за връзка, начин те да установят общи параметри за конфигуриране на канала спрямо техните възможности и изисквания. За тази цел се използва Session Description Protocol (SDP), който предоставя общ формат за предаване на възможности и изисквания към съответните параметри. SDP е текстово-базиран протокол и съобщенията му се пренасят чрез тялото на SIP съобщения.

## Структура на SIP съобщение

### SIP заявка

Примерна структура на една SIP заявка е показана на Фиг. 1.

INVITE sip:Marconi@radio.org SIP/2.0

Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b

Max-Forwards: 70

To: G. Marconi <sip:Marconi@radio.org>

From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341

Call-ID: j2qu348ek2328ws

CSeq: 1 INVITE

Subject: About That Power Outage...

Contact: <sip:n.tesla@lab.high-voltage.org>

Content-Type: application/sdp

Content-Length: 158

v=0

o=Tesla 2890844526 2890844526 IN IP4 lab.high-voltage.org

s=Phone Call

c=IN IP4 100.101.102.103

t=0 0

m=audio 49170 RTP/AVP 0

a=rtpmap:0 PCMU/8000

Фиг. 1

Всички SIP съобщения са в явен текст (plaintext). Това означава че в дефиницията на протокола тези съобщения се предават по канала точно по този начин без компресия.

Както при HTTP, SIP съобщението за заявка започва заглавна част. Тази част започва със метода или типа на заявката. В примера е използван метода INVITE. След това, на същият ред се записва и URI, което дефинира ресурсът към който трябва да се изпрати тази заявка. В края на редът се специфицира името и версията на протокола.

След заглавната част следва поредица от записи начени headers, разделени посредством CRLF (Carriage Return Line Feed) или нов ред. Всеки от тези записи е във формат ключ ‘:’ стойност. Като в стойността се позволяват всякакви символи с изключение на нов ред (CRLF). Някои записи могат да включват параметри в стойността си като параметрите ‘tag’ и ‘branch’ в примера на Фиг. 1.

След header частта следва тялото на SIP заявката. To е разделено от header частта със 2 CRLF. Както при HTTP, така и при SIP, тялото може да съдържа всякакви символи и обикновено съдържа някаква обща информация. Това практически показва че SIP съобщенията могат да пренасят всякаква информация в частта на тялото, без тя де е дефинирана в спецификацията на протокола. Най често при IMS комуникациите това е Session Description Protocol (SDP) протокола, който се използва за договаряне на параметрите на сесията.

### SIP отговор

Пример за SIP отговор е показан на Фиг. 2.

SIP/2.0 180 Ringing

Via: SIP/2.0/UDP lab.high-voltage.org:5060;branch=z9hG4bKfw19b

;received=100.101.102.103

To: G. Marconi <sip:marconi@radio.org>;tag=a53e42

From: Nikola Tesla <sip:n.tesla@high-voltage.org>;tag=76341

Call-ID: j2qu348ek2328ws

CSeq: 1 INVITE

Contact: <sip:marconi@tower.radio.org>

Content-length: 0

Фиг. 2

Структурата на SIP отговора не се различава много от структурата на заявката. Една от разликите тук е във заглавната част. За разлика от заявката в отговора заглавната част съдържа името и версията на протокола, код за отговора и кратко съобщение за отговор. Кодовете за отговор са стандартизирани и носят същото значение както при HTTP. Първата цифра на кода винаги определя класът на кода. В примера първата цифра е 1-ца което означава че сървърът връща информация като звънене. Съществуват много различни съобщения.

|  |  |  |
| --- | --- | --- |
| Клас | Определение | Действие |
| 1хх | Informational | Използва се за да предостави информация за състоянието на повикването. |
| 2хх | Success | Показва че заявката е била изпълнена успешно. |
| 3хх | Redirection | Указва на клиента да пренасочи заявката към друг URI. |
| 4хх | Client error | Обработката на заявката се е провалила заради грешка от страна на клиента. |
| 5хх | Server failure | Обработката на заявката се е провалила заради грешка от страна на сървъра. |
| 6хх | Global failure | Обработката на заявката се е провалила. |

Фиг. 3

Съобщението може да е произволен текст но си има и стандартизирани съобщения.

Въпреки че в това съобщение не се съдържа тяло (0 bytes body), в други отговори SIP сървъра може да върне информация към клиента посредством тялото.

### SIP методи

Тук са разписани някой от основните методи които се използват в SIP комуникацията

* INVITE – използва се за договаряне на сесия между user agents (UAs). Подобно на Initial Address Message (IAM) в ISUP.
* REGISTER – използва се за регистрация на агнета във SIP мрежата. Регистрацията е нужна за да може агента да приема входящи повиквания.
* BYE – използва се за прекратяване на съществуваща сесия. В телефонията това става когато потребителят затвори телефона.
* ACK – използва се за потвърждаване на потвърждението на, INVAITE съобщение, носейки информация за изискванията към сесията от викащата страна.
* CANCEL – Използва се за прекратяване на преговорите за сесия преди тя да е създадена.
* OPTIONS – използва се за да се получи информация за друг агент в мрежата. Изпраща се OPTIONS заявка към него.

## Видове SIP агенти

## Пример

# Архитектура на IP-based Multimedia Subsystem (IMS)

## Основни характеристики на IMS

IP мултимедийната подсистема или IP мултимедийната основна мрежова подсистема (IMS) е стандартизирана архитектурна рамка за предоставяне на IP мултимедийни услуги. Исторически погледнато, мобилните телефони са предоставяли услуги за гласови повиквания през мрежа в стил с комутационни вериги, а не строго през IP мрежа с комутиране на пакети. Алтернативни методи за предоставяне на глас като VoIP или други мултимедийни услуги са станали достъпни на смартфони, но те не са станали стандартизирани в цялата индустрия, IMS е архитектурна рамка, която осигурява такава стандартизация.

IP мултимедийна подсистема (IMS) представлява набор от спецификации, който описва мрежовата архитектура от ново поколение за внедряване на IP-базирана телефония и мултимедийни услуги. Тези спецификации определят цялостна рамка и архитектура, която позволява сближаването на технологиите за видео, глас, данни и мобилни мрежи.

Първоначално IMS е проектиран от организацията за безжични стандарти 3rd Generation Partnership Project (3GPP), като част от визията за развитие на мобилни мрежи извън GSM. Оригиналната му формулировка (3GPP Rel-5) представлява подход за предоставяне на интернет услуги през GPRS. Тази визия по-късно беше актуализирана от 3GPP, 3GPP2 и ETSI TISPAN, като изисква поддръжка на мрежи, различни от GPRS, като безжична LAN, CDMA2000 и фиксирани линии.

IMS използва IETF протоколи, когато е възможно, например протокола за започване на сесия (SIP). Според 3GPP IMS не е предназначен да стандартизира приложенията, а по-скоро да подпомага достъпа до мултимедийни и гласови приложения от безжични и кабелни терминали, т.е. да създаде форма на фиксирана-мобилна конвергенция (FMC). Това се прави чрез наличието на хоризонтален контролен слой, който изолира мрежата за достъп от слоя на услугите. От гледна точка на логическата архитектура, услугите не трябва да имат свои собствени функции за управление, тъй като контролният слой е общ хоризонтален слой. При изпълнение обаче това не означава непременно по-ниски разходи и сложност.

Алтернативните и припокриващи се технологии за достъп и предоставяне на услуги в кабелни и безжични мрежи включват комбинации от обща мрежа за достъп, софтсуичове и SIP.

Примери за глобални стандарти, базирани на IMS архитектура, са MMTel, който е основата за глас през LTE (VoLTE), Wi-Fi разговори (VoWIFI), видео през LTE (ViLTE), SMS/MMS през WiFi и LTE, USSD през LTE и Богати комуникационни услуги (RCS), които са известни още като joyn или Advanced Messaging, а сега RCS е реализация на телекомуникационните оператори.

Подсистемата на IP мултимедийната основна мрежа е съвкупност от различни функции, свързани чрез стандартизирани интерфейси, които са групирани в една IMS административна мрежа. Функцията не е възел (хардуерна кутия): Изпълнителят е свободен да комбинира две функции в един възел или да раздели една функция на два или повече възли. Всеки възел може също да присъства няколко пъти в една мрежа, за оразмеряване, балансиране на натоварването или организационни проблеми.

***Мрежа за достъп*** - потребителят може да се свърже с IMS по различни начини, повечето от които използват стандартния IP метод. IMS терминалите (като мобилни телефони, лични цифрови асистенти и компютри) могат да се регистрират директно в IMS, дори когато са в роуминг в друга мрежа или държава. Единственото изискване е те да могат да използват IP и SIP потребителски агенти. Фиксиран достъп (напр. цифрова абонатна линия (DSL), кабелни модеми, Ethernet, FTTx), мобилен достъп (например 5G NR, LTE, W-CDMA, CDMA2000, GSM, GPRS) и безжичен достъп (напр. WLAN, WiMAX) са поддържани технологии за достъп. Други телефонни системи, като обикновена стара телефонна услуга (POTS — старите аналогови телефони), H.323 и не-съвместими с IMS системи, се поддържат чрез gateway.

***Опорна мрежа*** – опорната мрежа на IMS е силно разгърната. Важно е да се отбележи че според спецификацията, функциите на тази мрежа не са посочени подробно. В този случай те са представени като абстрактни функционалности, които дефинират определено държание на опорната мрежа при различни събития но не обосновават как и чрез какви средства трябва да се постигне подобно държание. Например: как CSCF получава информация от базата данни?. Тази операция се реализира от оператора разработващ конкретната IMS система.

В следващите точки ще се разгледат подробно основните компоненти в опорната мрежа на IMS.

## Call Session Control Functions (CSCF)

Дефинирани са три вида контролни функции: Proxy-CSCF (P-CSCF), Serving-CSCF (S-CSCF) , Interrogating-CSCF (I-CSCF). Всяка функция си има своите специфични задачи. Общото между тях е че те участват по време на регистрацията и създаването на сесията и образуват SIP мрежата.

### Proxy Call Session Control Function (P-CSCF)

Proxy Call Session Control Function (P-CSCF) е входната точка на потребителските агенти в IMS. Това означава че всички SIP съобщения между потребителските агенти и произволна услуга в IMS ще преминават през P-CSCF. Може да се намира в чуждата (в пълни IMS мрежи) или в домашната мрежа (когато чуждата мрежа все още не е съвместима с IMS). Потребителският агент открива прокси функцията чрез DHCP, или чрез статична конфигурация (например по време на първоначално конфигуриране или чрез 3GPP IMS обект за управление).

Основните задачи които P-CSCF изпълнява са:

* SIP компресия – това позволява за по-бързо и по сигурно пренасяне на информацията през радио канала. Осъществява се от 3GPP.
* Реализиране IPSec/TLS протоколи с цел сигурност – позволява преносният канал между агента и прокси функцията да се криптира както и да се предостави вид автентикация чрез изпълнението на протокола IPSec или чрез TLS.
* Взаимодейства с Policy Decision Function (PDF) – позволява на прокси функцията да предоставя качество на канала спрямо заложената от оператора политика.
* Предоставя възможности за откриване на сесия в извънредни ситуации

### Interrogating Call Session Control Function (I-CSCF)

Използва се като обща точка, в мрежата на оператора, за всички връзки от вътрешни услуги към абонирани към тях потребителски агенти. IP адресът на тази функция се регистрира в DNS сървърът закачен към IMS мрежата, това позволява на всички вътрешни услуги лесно да го открият в мрежата.

I-CSCF изпълнява следните функции:

* При регистрация на потребителски агент в мрежата, тази функция трябва, чрез извличане на информация от Home Subscriber Server (HSS), да избере най-подходящият S-CSCF който да обслужва заявките на потребителския агент.
* Възможност да препраща SIP съобщения към услуга (приложение) или S-CSCF функция. Адресът на новият получател на съобщението се извлича от HSS.
* До Release 6 може да се използва и за скриване на вътрешната мрежа от външния свят (криптиране на части от SIP съобщението), в който случай се нарича Topology Hiding Inter-network Gateway (THIG). От версия 7 нататък тази функция "входна точка" е премахната от I-CSCF и вече е част от функцията за контрол на границата на междусистемата (IBCF). IBCF се използва като gateway към външни мрежи и осигурява NAT и Firewall функции. IBCF е граничен контролер на сесия, специализиран за интерфейса мрежа към мрежа (NNI).

### Serving Call Session Control Function (S-CSCF)

S-CSCF е централният възел на сигналната равнина. Той е SIP сървър, но изпълнява и контрол на сесията. Винаги се намира в домашната мрежа.

* Регистрация - Когато потребителски агент изпрати заявка за регистрация, тя се препраща към избран S-CSCF който трябва да изтегли информацията за автентикация от частният профил на клиента в HSS и да подтикне потребителският агент да се автентикира. След успешна автентификация, функцията изтегля списък за услугите които клиента може да достъпи.
* Контрол на услуги – след автентикацията, S-CSCF изтегля пълното множество от функции които потребителският агент може да достъпи както и със какво качество може да ги предостави. Това се нарича потребителски профил. Когато услуга иска да се свърже с потребителският агент или обратното. Всички SIP съобщеният преминават през S-CSCF който може да приложи съответната политика спрямо профила и да блокира достъпа на услуги които потребителският агент иска да достъпи.
* В IMS мрежата може да има голям брой S-CSCF тъй като те са най-често използваните и най-натоварените функции в мрежата. Поради това I-CSCF използва функции за балансиране на натоварването при избиране на S-CSCF.

Diagram, schematic

Description automatically generated

Фиг. 4

## Home Subscriber Server (HSS)

HSS е централната база данни, съхранявайки информация за всички абонати както и всякаква друга информация свързана с услугите които се предоставят от IMS. Основните записи включват потребителски идентификатори, информация нужна при регистрация, параметри за достъп както и информация за услугите които потребителят има право да ползва.

Частният потребителски идентификатор е въведен от оператора на домашната мрежа и може да се използва само в рамките на домашната мрежа. Използва се за автентификация при регистрация както и да определяне на правомощията за достъп на потребителският агент до съответните услуги.

Правомощията за достъп се използват при създаване на защитени сесии или такива изискващи допълнителна автентикация, автентикация по време на роуминг и д.р.

Публичният потребителски идентификатор е предназначен за използване от всякакви други услуги които искат да проверят информация за този потребител.

## Application Server (AS)

# CAMEL

# Session Description Protocol (SDP)

# Методи за информационна сигурност: IPSec/TLS

## Transport Security Layer (TLS)

## Internet Protocol Security (IPSec)

# IMS услуги глас, видео, данни

## IMS услуги

## Услуги, базирани на CAMEL

## IM-SSF

## Управление на GPRS сесии за данни

## Управление на SMS

## Управление на IP мултимедийни повиквания

# Изводи