

Министерство науки и высшего образования РФ
ФГБОУ ВО «Ульяновский государственный университет»
Факультет математики, информационных и авиационных технологий
Кафедра телекоммуникационных технологий и сетей

О. Л. Курилова, В.Г. Козловский, В.П. Смолеха

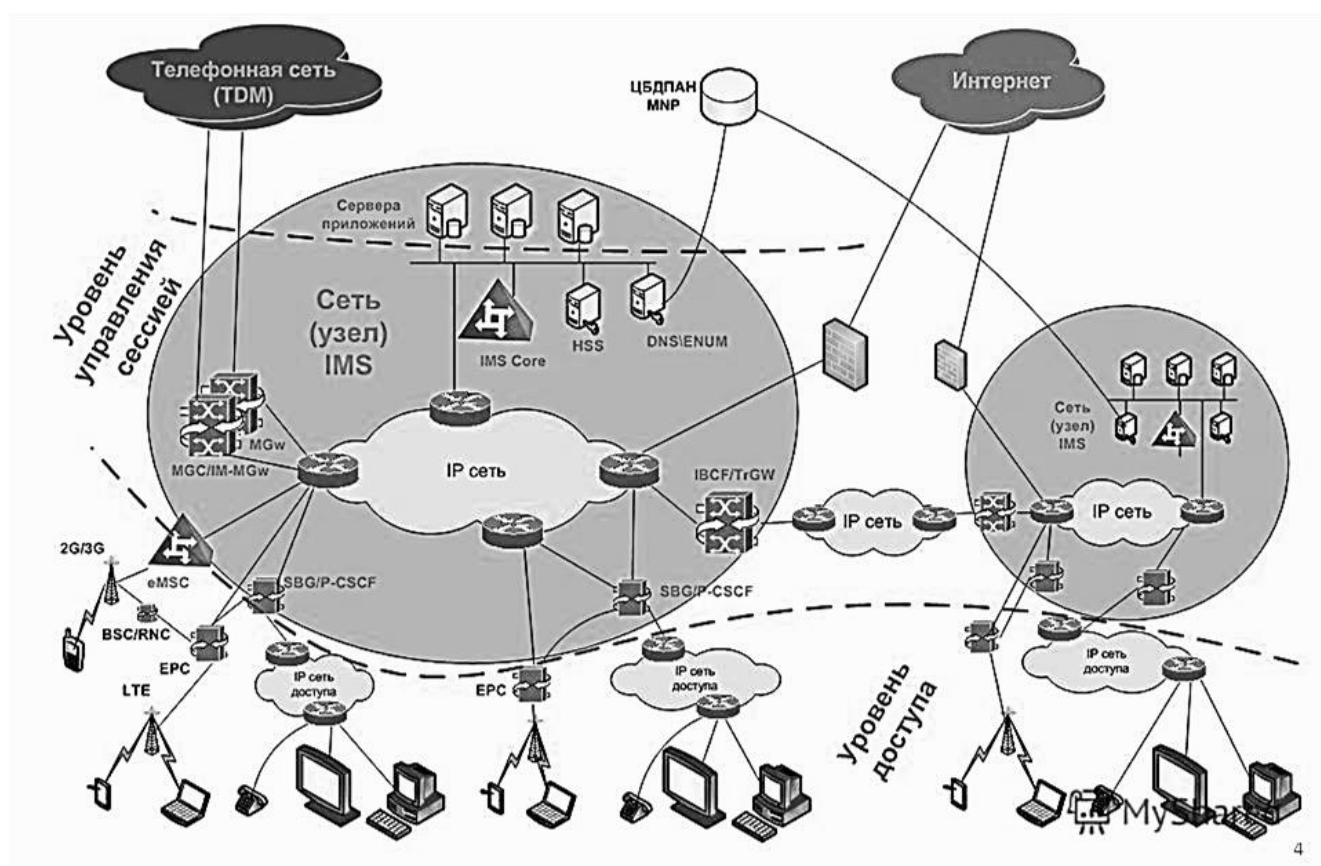
МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

для семинарских (практических) занятий и самостоятельной работы по
дисциплине

«Технология программной защиты в интернете»

для студентов направлений

09.03.02 «Информационные системы и технологии»



Методические рекомендации для семинарских (практических) занятий и самостоятельной работы по дисциплине «Инфокоммуникационные системы и сети» / составитель: О.Л. Курилова, В.Г. Козловский, В.П. Смолеха - Ульяновск: УлГУ, 2022 – 121 с.

Настоящие методические рекомендации предназначены для студентов направлений обучения 09.03.02 «Информационные системы и технологии». В работе приведены литература по дисциплине, темы дисциплины и вопросы в рамках каждой темы, рекомендации по изучению теоретического материала, контрольные вопросы для самоконтроля, задания для самостоятельной работы, задачи и упражнения для самостоятельной подготовки к семинарам или полностью самостоятельного освоения практических навыков, рекомендации по их выполнению.

Студентам всех форм обучения следует использовать данные методические рекомендации при подготовке к семинарам, самостоятельной подготовке, а также промежуточной аттестации по дисциплине «Инфокоммуникационные системы и сети».

Рекомендованы к введению в образовательный процесс

Учёным советом факультета математики, информационных и авиационных технологий УлГУ

протокол № 3 /22 от «19» апреля 2022 г.

Содержание

Введение	4
Часть 1. «Сети NGN. Администрирование IP PBX Asterisk»	6
1.1 Файлы конфигурации IP PBX Asterisk. Предварительная настройка IP PBX Asterisk	7
Предварительная настройка IP PBX Asterisk	7
Создание абонента и настройка маршрутизации	8
Последовательность создания пользователей в web-интерфейсе:	10
1.2 Лабораторная работа №1 «Создание абонента и настройка маршрутизации»	12
1.3 Лабораторная работа №2 «Услуга “Точное время»	17
1.4 Лабораторная работа №3 «Настройка маршрутизации между двумя IP PBX Asterisk»	23
1.5 Лабораторная работа №4 «Настройка маршрутизации между двумя IP PBX Asterisk (АТС и УПАТС)»	26
1.6 Лабораторная работа №5 «Настройка маршрутизации с установлением видеосвязи»	31
1.7 Лабораторная работа №6. «Анализ качества передачи речи по IP-сети»	34
1.8 Лабораторная работа №7. «Построение сети связи. Районированная ГТС без узлообразования»	39
1.9 Лабораторная работа №8. «Построение сети связи. Районированная ГТС без узлообразования с узлом УСС»	43
1.10 Лабораторная работа №9. «Построение сети связи. Организация сети при соединении двух АМТС, расположенных в разных городах»	52
Часть 2. «Сети NGN. Оборудование IMS»	67
Лабораторная работа №1 «Процедура регистрации»	67
Лабораторная работа №2 «Сети NGN. Оборудование IMS. Типы сессий в IMS»	73
Лабораторная работа №3 «Мультимедийные сессии»	82
Лабораторная работа №4 «Дополнительные услуги»	86
Лабораторная работа №5 «Неудачные попытки установления мультимедийных сессий»	96
Приложение 1. Создание пользователя, зарегистрированного на сервере Asterisk, в программном телефоне Twinkle	102
Приложение 2. Создание пользователя, зарегистрированного на сервере Asterisk, в программном телефоне Linphone	104
Приложение 3. Работа в терминале	108
Приложение 4. Создание абонента и настройка маршрутизации в IP PBX Asterisk	114
Приложение 5. Настройка аудио выхода	117
Приложение 6. Содержимое файлов конфигурации с пояснениями	118
Список информационных источников	121

Введение

В интерактивном лабораторном классе телекоммуникационных протоколов и технологий используется аппаратно-программный комплекс (АПК) СОТСБИ, в котором реализован комплексный подход к системе обучения.

Аппаратно-программный комплекс состоит из:

- сервера учебных курсов СОТСБИ-У;
- сервера для выполнения лабораторных работ СОТСБИ-NGN;
- рабочих мест учащихся;
- рабочего места преподавателя.

Этапы обучения в АПК СОТСБИ включают в себя:

- изучение теоретического материала, состоящего из анимированных слайдов с текстовым пояснением в СОТСБИ-У;
- тестирование в СОТСБИ-У;
- моделирование – практические работы в СОТСБИ-У;
- зачет в СОТСБИ-У;
- выполнение лабораторных работ в СОТСБИ-NGN.

Целью лабораторного практикума является формирование у студентов системы знаний по выполнению лабораторных работ в СОТСБИ-NGN.

Изучение лабораторного практикума базируется на успешно усвоенных базовых понятиях дисциплин математического и естественно-научного цикла и дисциплин профессионального цикла: «Информатика», «Операционные системы и среды», «Архитектура информационных систем».

Каждая лабораторная работа включает подробное описание последовательности действий исполнителя с множеством рисунков.

Лабораторные работы представлены в виде двух частей.

Первая часть «Сети NGN. Администрирование IP PBX Asterisk» включает в себя:

- Обзор и настройку файлов конфигурации IP PBX Asterisk.
- Предварительная настройка IP PBX Asterisk
- Создание абонента и настройка маршрутизации
- Последовательность создания пользователей в web-интерфейсе.
- Лабораторная работа №1 «Создание абонента и настройка маршрутизации»
- Лабораторная работа №2 «Услуга “Точное время»
- Лабораторная работа №3 «Настройка маршрутизации между двумя IP PBX Asterisk»
- Лабораторная работа №4 «Настройка маршрутизации между двумя IP PBX Asterisk (АТС и УПАТС)»
- Лабораторная работа №5 «Настройка маршрутизации с установлением видеосвязи»
- Лабораторная работа №6. «Анализ качества передачи речи по IP-сети»
- Лабораторная работа №7. «Построение сети связи. Районированная ГТС без узлообразования»
- Лабораторная работа №8. «Построение сети связи. Районированная ГТС без узлообразования с узлом УСС».
- Лабораторная работа №9. «Построение сети связи. Организация сети при соединении двух АМТС, расположенных в разных городах».

Вторая часть «Сети NGN. Оборудование IMS» включает в себя пять лабораторных работ:

- Лабораторная работа №1 «Процедура регистрации»
- Лабораторная работа №2 «Сети NGN. Оборудование IMS. Типы сессий в IMS»
- Лабораторная работа №3 «Мультимедийные сессии»
- Лабораторная работа №4 «Дополнительные услуги»

- Лабораторная работа №5 «Неудачные попытки установления мультимедийных сессий»

Лабораторный практикум содержит шесть приложений:

- Приложение 1. Создание пользователя, зарегистрированного на сервере Asterisk, в программном телефоне Twinkle.
- Приложение 2. Создание пользователя, зарегистрированного на сервере Asterisk, в программном телефоне Linphone.
- Приложение 3. Работа в терминале.
- Приложение 4. Создание абонента и настройка маршрутизации в IP PBX Asterisk
- Приложение 5. Настройка аудио выхода.
- Приложение 6. Содержимое файлов конфигурации с пояснениями
- Список информационных источников.

Лабораторный практикум подготовлен на кафедре «Телекоммуникационных технологий и сетей».

Методические рекомендации по выполнению лабораторных работ будут интересны и полезны для студентов вузов, обучающихся по специальностям в области информационных технологий и сетей, преподавателям и специалистам в области построения компьютерных сетей, сетей связи и IP-телефонии.

Выражаем благодарность студентам ФМИАТ УЛГУ Никифорову И.В. и Ростову М.А. за активное участие в практической реализации данного лабораторного практикума.

Часть 1. «Сети NGN. Администрирование IP PBX Asterisk»

Все работы будут проходить на базе полигона СОТСБИ-NGN, расположенного в интерактивно-лабораторном учебном классе «Телекоммуникационных технологий и протоколов» (аудитория 2/24а) в УлГУ (Рисунок 1). При выполнении работ будут задействованы рабочие машины (РМ) №1-10.



Рисунок 1 – Интерактивно-лабораторный учебный класс

Сеть VoIP полигона СОТСБИ-NGN, используемая для проведения лабораторных и исследовательских занятий, состоит из следующих основных элементов:

- сервер IP PBX Asterisk;
- сервер GnuGK;
- сервер Протей-МКД (mCore.MKD);
- серверы OpenIMSCore (P-CSCF, I-CSCF, S-CSCF);
- сервер базы данных пользователей OpenIMSCore HSS;
- сервер приложений (Presence Server);
- рабочие места учащихся (РМ), оборудованные периферийными устройствами для приема и передачи мультимедийной информации (гарнитура и видеочасть).

Кроме того, за каждым РМ закреплен собственный сервер IP PBX Asterisk, установленный непосредственно на РМ.

Задания выполняются с использованием программных телефонов Twinkle, Ekiga и Linphone.

Все изменения, внесенные в работу рабочего места (РМ), действует только в течение сессии. После перезагрузки система возвращается в исходное состояние.

Программные телефоны, используемые на полигоне СОТСБИ-NGN, могут работать в двух режимах: с регистрацией на SIP-сервере и в режиме «точка-точка».

При работе телефона через SIP-сервер, сервер занимается обслуживанием входящих и исходящих вызовов, осуществленных с помощью этого телефона. В этом случае все сообщения протокола SIP, сгенерированные в процессе обслуживания вызова, обрабатываются SIP-сервером. Данные о SIP-сервере должны быть указаны в настройках телефона. Информация об абоненте может быть представлена либо непосредственно в виде номера абонента, либо в виде имени пользователя, либо в виде URI пользователя (в формате *имя_пользователя@адрес_sip-*

сервера).

В режиме «точка-точка» связь с удаленным терминалом осуществляется напрямую. В этом случае все сообщения протокола транслируются непосредственно между телефонами. Для организации вызова в режиме «точка-точка» необходимо знать текущие IP-адреса терминалов. В качестве данных вызываемого абонента в этом случае будет использоваться IP-адрес вызываемого абонента.

Перед началом выполнения лабораторной работы необходимо настроить звуковые устройства (см. раздел «Настройка звука» в [11]).

Если между двумя программными телефонами установлено соединение, но звук отсутствует, необходимо проверить в настройках программы используемые кодеки (для некоторых программных телефонов не все типы кодеков совместимы друг с другом) и выбранное звуковое устройство.

Настоятельно рекомендуется запускать другой программный телефон только после полного закрытия предыдущего. При одновременном запуске двух программных телефонов, последний может выдать сообщение о том, что порт 5060 для сигнализации SIP занят другим приложением, и тогда требуется корректно завершить работу всех запущенных программных телефонов или перезагрузить РМ.

Также перед началом выполнения лабораторной работы необходимо подключить пользовательский каталог (см. Приложении 2 к [11]) для возможности сохранений файлов в личную папку.

1.1 Файлы конфигурации IP PBX Asterisk. Предварительная настройка IP PBX Asterisk

Предварительная настройка IP PBX Asterisk

На каждом РМ установлен собственный сервер Asterisk. Нумерация на сервере пятизначная, формата 1-XX-YY, где XX — номер РМ (01, 02 и т.д.), YY — порядковый номер абонента (00–99).

При выполнении лабораторных работ используется эмулятор терминала *lterminal*, запуск которого осуществляется с помощью ярлыка «Управление Aslterisk CLI». Для удобства использования консоли добавлена возможность работы с несколькими вкладками эмулятора терминала одновременно. Открыть дополнительную вкладку можно комбинацией клавиш `<Ctrl>+<Shift>+<t>`.

Файлы конфигурации Asterisk расположены в каталоге `/etc/asterisk` и имеют расширение `*.conf`. В ходе выполнения практических работ, учащиеся редактируют эти файлы при помощи, например, встроенного текстового редактора в *mc* (*Midnight Commander*). Для запуска *Midnight Commander* в консоли необходимо ввести команду `mc`. В открывшемся файловом менеджере навигация осуществляется с помощью стрелок клавиатуры, переход на уровень выше — через каталог `/...`. Файлы с расширением `*.conf.bkup` являются резервными копиями файлов конфигурации и не предназначены для редактирования.

После выполнения лабораторной работы исправленные файлы конфигурации могут быть сохранены на NFS сервере в индивидуальном каталоге учащегося.

При проведении всех работ с IP PBX Asterisk, установленной на рабочем месте, используется сетевой интерфейс `eth0:0`. IP адрес этому интерфейсу назначается автоматически согласно номеру РМ (рабочее место). Выяснить присвоенный IP адрес можно с помощью утилиты *ifconfig* (Рисунок 2).

```

root@rm-09:~# ifconfig
eth0      Link encap:Ethernet  HWaddr d8:cb:8a:01:0b:b0
          inet addr:172.16.119.9  Bcast:172.16.119.255  Mask:255.255.252.0
          inet6 addr: fe80::dacb:8aff:fe01:bb0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:936173 errors:0 dropped:0 overruns:0 frame:0
          TX packets:46334 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1412315117 (1.4 GB)  TX bytes:4637508 (4.6 MB)

eth0:0    Link encap:Ethernet  HWaddr d8:cb:8a:01:0b:b0
          inet addr:172.16.119.159  Bcast:172.16.119.255  Mask:255.255.252.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Локальная петля (Loopback)
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:149 errors:0 dropped:0 overruns:0 frame:0
          TX packets:149 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:10505 (10.5 KB)  TX bytes:10505 (10.5 KB)

wlan0     Link encap:Ethernet  HWaddr b8:86:87:85:24:c6
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

```

Рисунок 2 – Ответ на утилиту *ifconfig*.

Перед началом работы необходимо открыть для редактирования файл */etc/asterisk/sip.conf* через утилиту «Управление Asterisk CLI», которая запускает эмулятор терминала *Ixterminal* с правами суперпользователя.

Создание абонента и настройка маршрутизации

IP PBX Asterisk работает с использованием конфигурационных файлов. На данном этапе потребуется изменить настройки, хранящиеся в файлах */etc/asterisk/sip.conf* и */etc/asterisk/extensions.conf*. Файл *sip.conf* содержит описание базовых параметров работы протокола SIP, настройки NAT, перечень используемых кодеков, учетных записей абонентов и т.д. Файл *extensions.conf* описывает правила обработки вызовов поступающих в систему.

Последовательность выполнения работы:

1. Запустить утилиту «Управление Asterisk CLI».
2. Выполнить команду *mc* — откроется файловый менеджер. Перейти на уровень выше */..* и открыть для редактирования файл */etc/asterisk/sip.conf*
3. В секции *[general]* изменить значение параметра *udpbindaddr* на IP адрес интерфейса *eth0:0* (Рисунок 3), т. е. на адрес Вашего компьютера. Сохранить изменения в файле.

```

sip.conf      [----] 0 L: [ 1+ 3  4/  4] *(36 / 36b) <EOF>
[general]
udpbindaddr=172.16.119.1

```

Рисунок 3 – Изменение файла *sip.conf*

4. Выйти из редактирования файла в файловый менеджер, затем выйти из файлового менеджера в консольный режим.

5. Запустить процесс *asterisk* командой */etc/init.d/asterisk start*.

Удостовериться, что процесс *asterisk* запущен и прослушивает порт 5060 командой *netstat -nlpu | grep 5060* (Рисунок 4).

```
root@rm-01:~# /etc/init.d/asterisk start
Starting Asterisk PBX: asterisk.
root@rm-01:~# netstat -nlpu | grep 5060
udp        0      0 172.16.119.1:5060      0.0.0.0:*
4268/asterisk
root@rm-01:~#
```

Рисунок 4 – Запуск процесса *asterisk*

6. Сохранить и выйти в файловый менеджер.

7. Открыть для редактирования файл */etc/asterisk/sip.conf* и добавить двух абонентов с номерами 1-01-00 и 1-01-01. Пример содержимого файла (Рисунок 5):

```
[general]
allowguest=no
udpbindaddr=ip_addr_eth0:0 - Ваш адрес
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
[sip_sub](!) - Ваш адрес
type=friend
host=dynamic
context=internal
disallow=all
allow=alaw
[10100](sip_sub) – адреса пользователей, с которыми будет происходить звонок
[10101](sip_sub) - Ваш адрес
```

```
sip.conf
[general]
allowguest=no
udpbindaddr=172.16.119.1
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
[172.16.119.1](!)
type=friend
host=dynamic
context=internal
disallow=all
allow=alaw
[10100](172.16.119.2)
[10101](172.16.119.1)
```

Рисунок 5 – Изменения файла *sip.conf*

8. Сохранить изменения файла *sip.conf* и из файлового менеджера в файл */etc/asterisk/extensions.conf* добавить правило обработки вызовов:

```
[general]
```

```
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 10100,1,Dial(SIP/${EXTEN})
exten => 10100,n,Hangup()
exten => 10101,1,Dial(SIP/${EXTEN})
exten => 10101,n,Hangup()
```

9. Перезапустить процесс asterisk командой `/etc/init.d/asterisk restart`.

10. С помощью команды `asterisk -rvvv` подключиться к консоли управления Asterisk. (Рисунок 6)

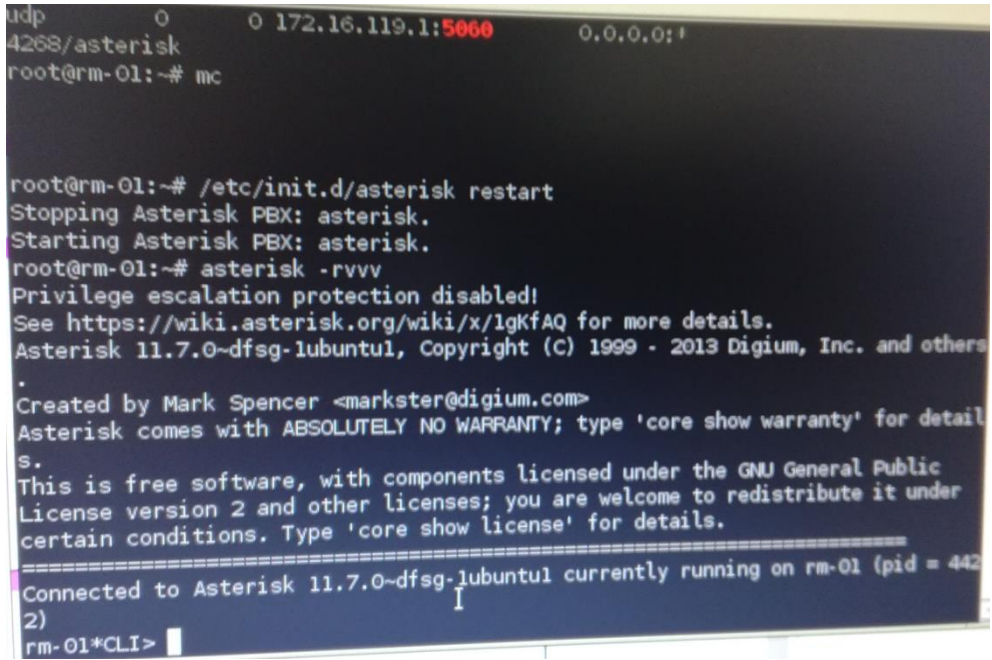


Рисунок 6 – Консоль управления Asterisk

11. Открыть web-интерфейс IP PBX Asterisk и создать в нем два новых абонента с параметрами, указанными в предыдущих шагах.

Последовательность создания пользователей в web-интерфейсе:

Запуск и работа с Asterisk

Управление IP PBX Asterisk может осуществляться посредством веб-интерфейса. Для запуска веб-интерфейса необходимо нажать на ярлык Управление Asterisk.

В окне браузера появится окно авторизации пользователя (Рисунок 7), в котором необходимо ввести логин и пароль, которые пользователь использовал при работе с учебным курсом СОТСБИ-У.

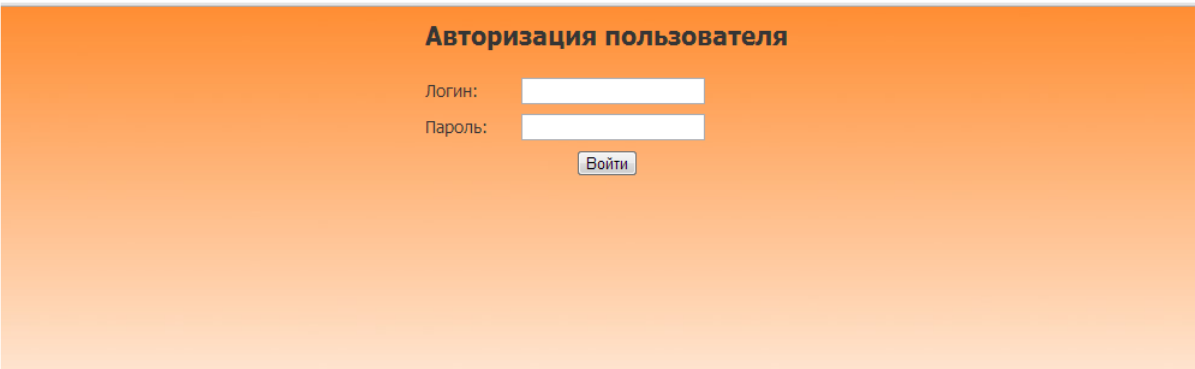


Рисунок 7 – Окно авторизации пользователя

В случае ввода неверного логина или пароля отображается страница с соответствующим сообщением.

После авторизации пользователя появляется главная страница графического интерфейса IP PBX Asterisk (Рисунок 8). В левой части страницы перечислены основные пункты меню.

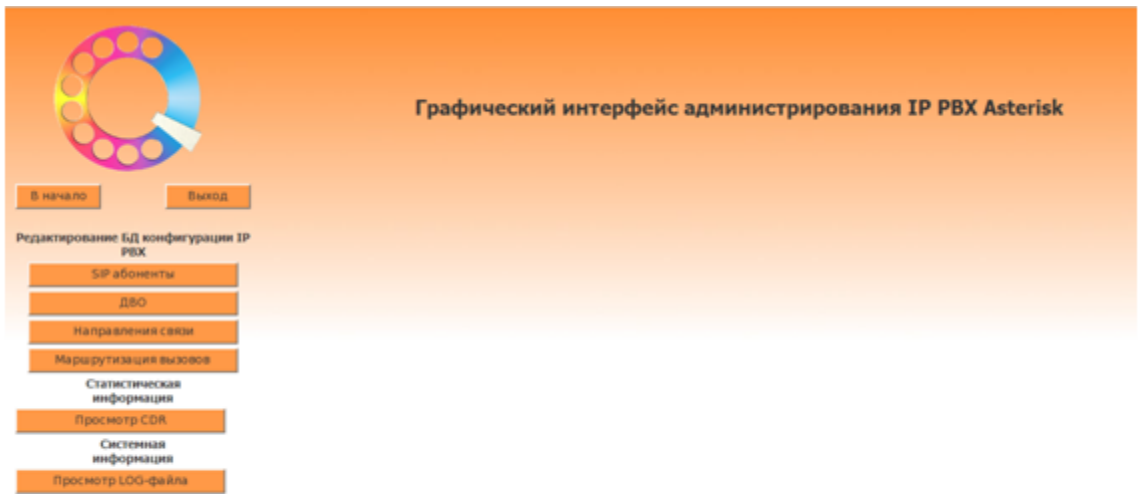


Рисунок 8 – Графический интерфейс IP PBX Asterisk

Редактирование БД конфигурации IP PBX Asterisk

Представленный графический интерфейс позволяет редактировать параметры SIP абонентов (тип абонента, разрешенные кодеки, возможность поддержки видеовызова и т.д.). Для работы с базой данных SIP абонентов необходимо выбрать пункт меню «SIP абоненты» в соответствующем разделе. В данном разделе отображаются только создаваемые абоненты (Рисунок 9), а не все абоненты, зарегистрированные на Asterisk.

Управление SIP абонентами IP PBX Asterisk

Редактирование данных

Вставка данных

Удаление данных

Общее количество SIP абонентов в БД: 2

1

	Номер абонента	Тип абонента	Идентификационная строка абонента (CALLERID)	Порт сигнализации SIP	Разрешенные кодеки	Количество одновременных вызовов	Поддержка видеовызовов	Проксирование RTP
☒	10100	friend	10100	5060	alaw ulaw g722 gsm speex speex16 h261 h263 h263p	1	no	no
☐	10101	friend	10101	5060	alaw ulaw g722 gsm speex speex16 h261 h263 h263p	1	no	no

Рисунок 9 – Список абонентов

Для создания новой записи об абоненте необходимо нажать кнопку «Вставка данных» (Рисунок 10), при этом появится пустая форма ввода данных; в левом столбце перечислены названия полей абонентской записи, центральный столбец содержит текстовые поля и выпадающие списки для установки значений параметров абонентской записи, правый столбец содержит пиктограммы "?", при наведении на них указателя мыши появляются подсказки с краткими пояснениями по каждому параметру абонентской записи.

После добавления новой абонентской записи не требуется перезапуска IP PBX Asterisk, информация из базы данных автоматически считывается IP PBX Asterisk.



Рисунок 10 – Вставка абонентских данных

1.2 Лабораторная работа №1 «Создание абонента и настройка маршрутизации»

IP PBX Asterisk, как и большинство приложений, работает с использованием конфигурационных файлов. На данном этапе потребуется изменить настройки хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`. Файл `sip.conf` содержит описание базовых параметров работы протокола SIP, настройки NAT, перечень используемых кодеков, учетных записей абонентов и т.д. Файл `extensions.conf` описывает правила обработки вызовов поступающих в систему.

1. Открыть для редактирования файл `/etc/asterisk/sip.conf` и добавить двух абонентов с номерами `1-XX-00` и `1-XX-01`, например для PM2 (Рисунок 11).

```
/etc/asterisk/sip.conf
[general]
allowguest=no
udpbindaddr=172.16.119.152
transport=udp
stvllookup=yes
disallow=all
allow=alaw
allow=ulaw
[172.16.119.152](!)
tupe=friend
host=dynamic
context=internal
disallow=all
allow=alaw
[10200](172.16.119.152)
[10201](172.16.119.152)
```

Рисунок 11 – Редактирование файла `sip.conf`

2. В файл `/etc/asterisk/extensions.conf` добавить правило обработки вызовов (Рисунок 12):

```

extensions.conf [BM--] 23 L:
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten=>10200,1,Dial(SIP/${EXTEN})
exten=>10200,n,Hangup()
exten=>10201,1,Dial(SIP/${EXTEN})
exten=>10201,n,Hangup()

```

Рисунок 12 – Редактирование файла *extensions.conf*

3. Перезапустить процесс *asterisk* командой */etc/init.d/asterisk /etc/init.d/asterisk /etc/init.d/asterisk restart*.

4. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (Рисунок 13).

```

3349/asterisk
root@rm-09:~# nano /etc/asterisk/sip.conf
root@rm-09:~# nano /etc/asterisk/extensions.conf
root@rm-09:~# nano /etc/asterisk/sip.conf
root@rm-09:~# /etc/init.d/asterisk restart
Stopping Asterisk PBX: asterisk.
Starting Asterisk PBX: asterisk.
root@rm-09:~# asterisk -rvvv
Privilege escalation protection disabled!
See https://wiki.asterisk.org/wiki/x/1gKfAQ for more details.
Asterisk 11.7.0~dfsg-lubuntu1, Copyright (C) 1999 - 2013 Digium, Inc. and others
.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 11.7.0~dfsg-lubuntu1 currently running on rm-09 (pid = 371
9)
rm-09*CLI>

```

Рисунок 13 – Подключение к консоли управления Asterisk

5. На РМ запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» изменить порт *UDP 5062*, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером *1-XX-00* (Рисунок 14, Рисунок 15).

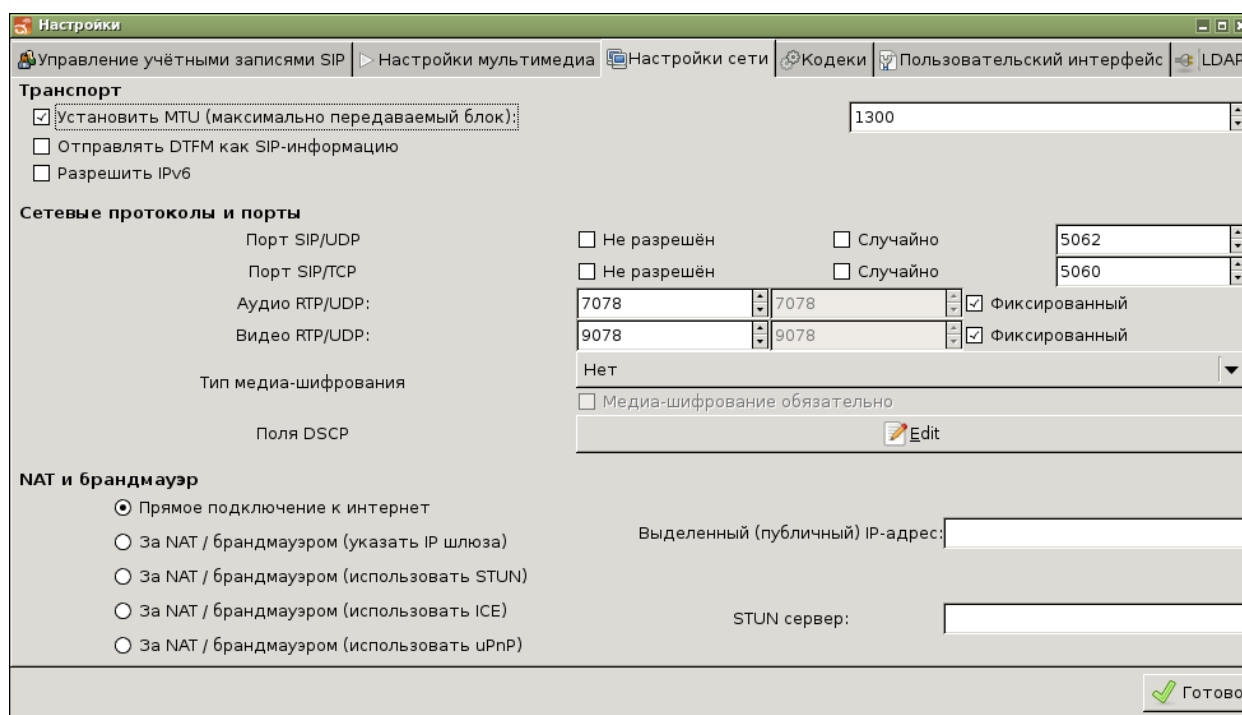


Рисунок 14 – Настройка программного телефона Linphone

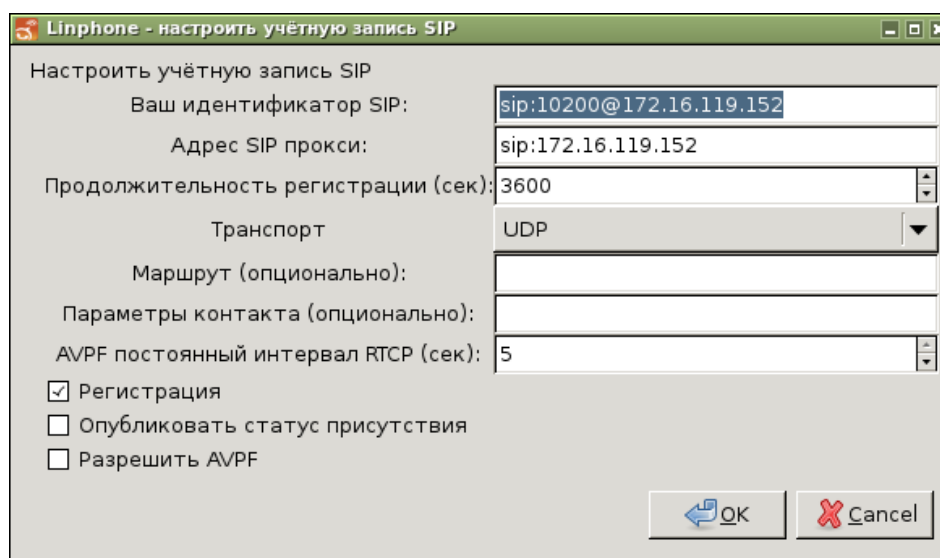


Рисунок 15 – Настройка учетной записи программного телефона Linphone

После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента (Рисунок 16).

Пример сообщения:

-- Registered SIP '10200' at 172.16.119.2:5062

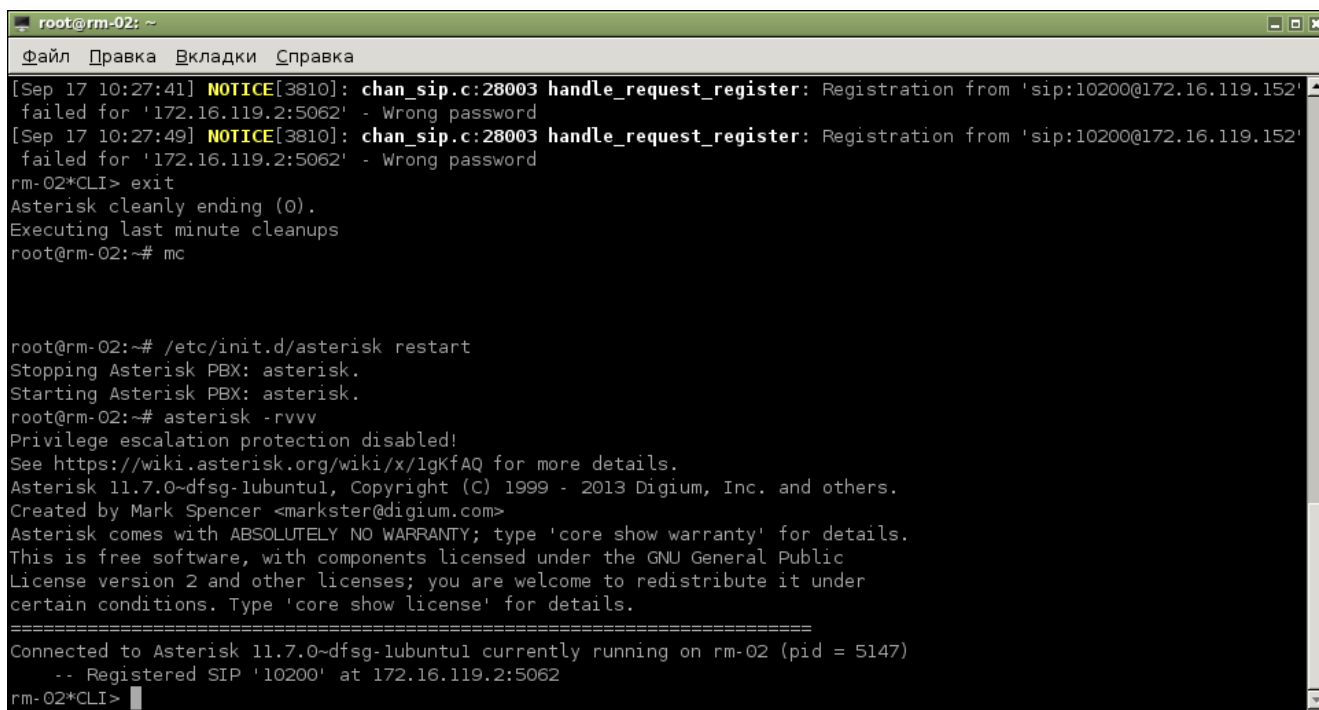


Рисунок 16 – Успешная регистрация абонента

6. На РМ запустить программный телефон Twinkle. В мастере создания учетных записей указать номер 1-XX-01. В системных настройках определить SIP порт, например, 5063 (Рисунок 17, Рисунок 18).

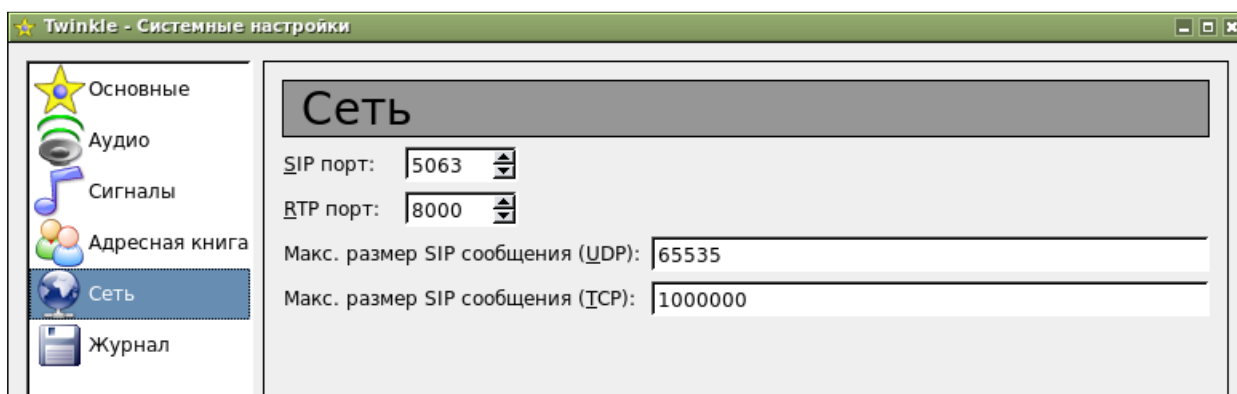


Рисунок 17 – Настройка программного телефона Twinkle.

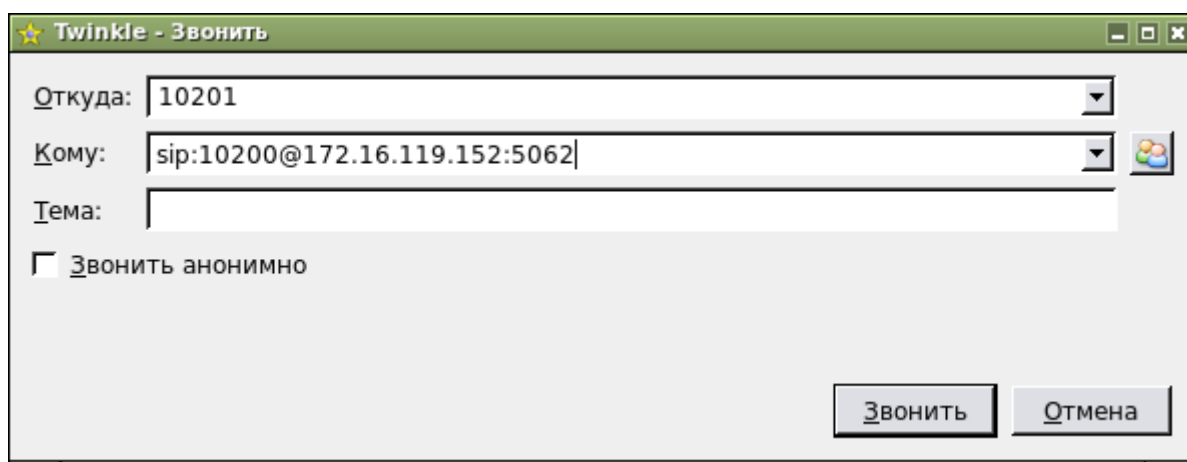


Рисунок 18 – Настройка профиля пользователя в программном телефоне Twinkle.

После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента (Рисунок 19).

```
root@rm-02: ~
Файл  Правка  Вкладки  Справка
root@rm-02:~# asterisk -rvvv
Privilege escalation protection disabled!
See https://wiki.asterisk.org/wiki/x/1gKfAQ for more details.
Asterisk 11.7.0~dfsg-1ubuntu1, Copyright (C) 1999 - 2013 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 11.7.0~dfsg-1ubuntu1 currently running on rm-02 (pid = 5147)
-- Registered SIP '10201' at 172.16.119.2:5063
rm-02*CLI>
```

Рисунок 19 – Успешная регистрация абонента

7. Выполнить контрольный вызов между абонентами 1-XX-00 и 1-XX-01. В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова. Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и маршрутизации. Выход из консоли управления Asterisk осуществляется командой *exit*. Пример отчета об успешной обработке вызова (Рисунок 20, Рисунок 21):

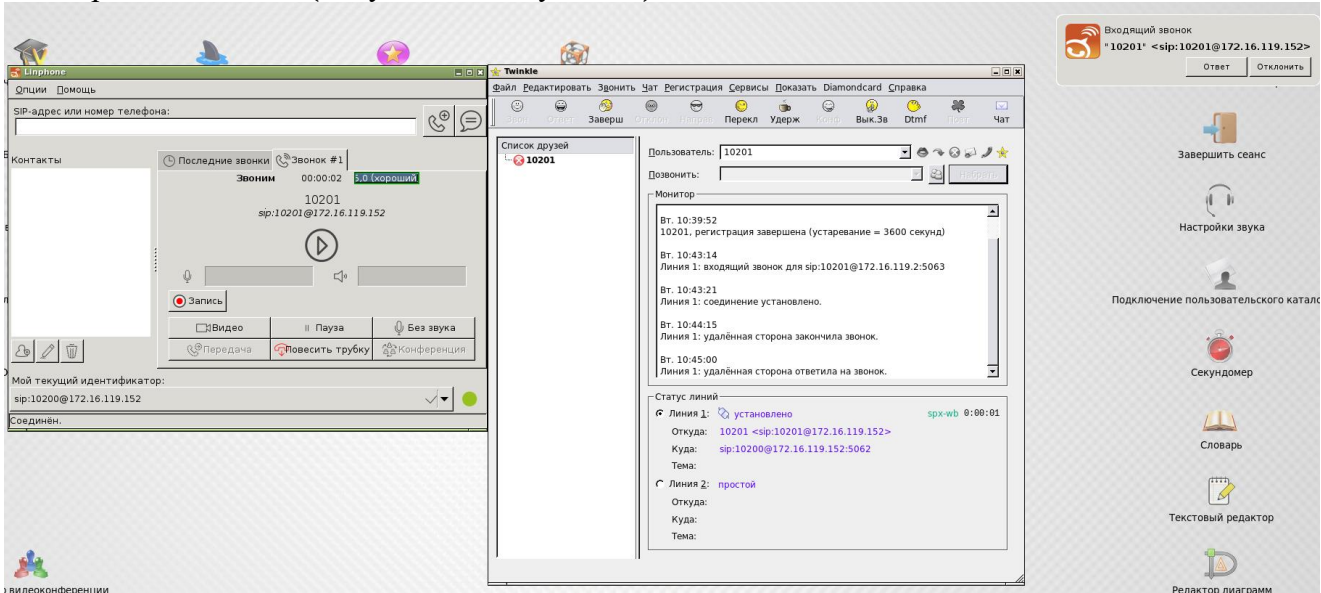


Рисунок 20 – Успешная обработка вызова

```
root@rm-02: ~
Файл Правка Вкладки Справка

== Using SIP RTP CoS mark 5
-- Executing [10201@internal:1] Dial("SIP/10200-00000004", "SIP/10201") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/10201
-- SIP/10201-00000005 is ringing
-- Got SIP response 603 "Decline" back from 172.16.119.2:5063
-- SIP/10201-00000005 is busy
== Everyone is busy/congested at this time (1:1/0/0)
-- Executing [10201@internal:2] Hangup("SIP/10200-00000004", "") in new stack
== Spawn extension (internal, 10201, 2) exited non-zero on 'SIP/10200-00000004'
== Using SIP RTP CoS mark 5
-- Executing [10201@internal:1] Dial("SIP/10200-00000006", "SIP/10201") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/10201
-- SIP/10201-00000007 is ringing
-- SIP/10201-00000007 answered SIP/10200-00000006
-- Remotely bridging SIP/10200-00000006 and SIP/10201-00000007
== Spawn extension (internal, 10201, 1) exited non-zero on 'SIP/10200-00000006'
rm-02*CLI>
```

Рисунок 21 – Отчет об успешной обработке вызова в консоли.

8. Скопировать файлы конфигурации `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf` на NFS сервер в индивидуальный каталог учащегося.

1.3 Лабораторная работа №2 «Услуга «Точное время»

Служба «Точное время» предоставляет услугу, которая позволяет оперативно получать информацию о точном времени региона, в котором находится абонент.

Будет описана настройка маршрутизации на РМ №10 между программным телефоном Linphone и службой «Точное время».

На (Рисунок 22) изображена схема маршрутизации между программным телефоном и службой «Точное время», а в таблице 1 приведены номера абонентов программного телефона и службы «Точное время». Детализированный алгоритм настройки маршрутизации между программным телефоном и службой «точное время» в графическом виде представлен на Рисунок 23.

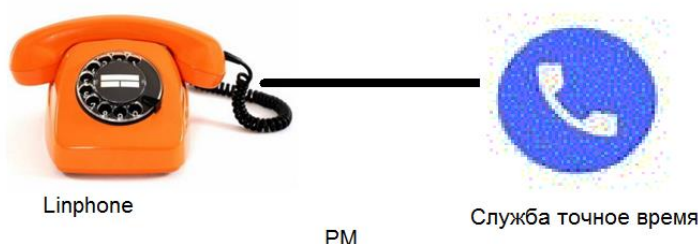


Рисунок 22 – Схема маршрутизации между программным телефоном и службой «Точное время»

Таблица 1. Номера программного телефона и службы «Точное время»

Программный телефон / Служба	Номер
Программный телефон Linphone	11000
Программный телефон Linphone	11001
Служба «Точное время»	060



Рисунок 23 – Алгоритм настройки маршрутизации между программным телефоном и службой «Точное время»

Алгоритм выполнения работы:

- 1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).
- 2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).
- 3. Для настройки маршрутизации необходимо изменить настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).
- 4. Открыть для редактирования файл `/etc/asterisk/sip.conf` и добавить двух абонентов с номерами `11000` и `11001` (`1VV00` и `1VV01`, где `VV` это номер РМ, например, РМ №10 имеет номер 10). Пример содержимого файла:

sip.conf (шаблон)

```
[general]
allowguest=no
udpbindaddr=172.16.119.X
transport=udp
srvlookup=yes
disallow = all
allow = alaw
allow = ulaw

[172.16.119.X](!)
type=friend
host=dynamic
```

sip.conf (РМ №10)

```
[general]
allowguest=no
udpbindaddr=172.16.119.10
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw

[172.16.119.10](!)
type=friend
host=dynamic
```

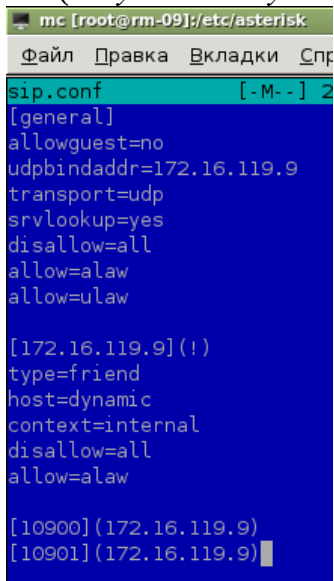
```
context= internal
disallow = all
allow = alaw
```

```
context=internal
disallow=all
allow=alaw
```

```
[1VV00](172.16.119.X)
[1VV01](172.16.119.X)
```

```
[11000](172.16.119.10)
[11001](172.16.119.10)
```

В шаблоне файла sip.conf вместо символов X прописывается последнее число IP-адреса РМ; V – цифры, обозначающие номера РМ (Рисунок 24Рисунок 25).



```
mc [root@rm-09]:/etc/asterisk
Файл  Правка  Вкладки  Спр
sip.conf  [-М- -] 2
[general]
allowguest=no
udpbinding=172.16.119.9
transport=udp
srlookup=yes
disallow=all
allow=alaw
allow=ulaw

[172.16.119.9](!)
type=friend
host=dynamic
context=internal
disallow=all
allow=alaw

[10900](172.16.119.9)
[10901](172.16.119.9)
```

Рисунок 24 – Изменение файла sip.conf

5. В файлы /etc/asterisk/extensions.conf добавить правила обработки вызовов: extensions.conf (шаблон):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 1VV00,1,Dial(SIP/${EXTEN})
exten => 1VV00,n,Hangup()
exten => 1VV01,1, Dial(SIP/${EXTEN})
exten => 1VV01,n,Hangup()
exten => 060,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja)
exten => 060,n,SayUnixTime(,HM)
exten => 060,n,Hangup()
```

extensions.conf (РМ №10):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
```

```

exten => 11000,1,Dial(SIP/${EXTEN})
exten => 11000,n,Hangup()
exten => 11001,1,Dial(SIP/${EXTEN})
exten => 11001,n,Hangup()
exten => 060,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja)
exten => 060,n,SayUnixTime(,HM)
exten => 060,n,Hangup()

```

В шаблоне файла *extensions.conf* вместо символов VV прописываются цифры, обозначающие номера РМ.

Содержание файлов конфигурации подробно описано в приложении 6.

Команда *Playback()* воспроизводит в канале предварительно записанный звуковой файл.

В качестве аргумента задается имя воспроизводимого файла и полный путь к нему (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja).

Команда *SayUnixTime* показывает точное время.

Команда *Hangup* нужна для разъединения активного канала.

6. Перезапустить процесс asterisk командой */etc/init.d/asterisk restart* (Рисунок 25).

7. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (Рисунок 25).

```

root@rm-09: ~
Файл Правка Вкладки Справка

root@rm-09:~# mc

root@rm-09:~# /etc/init.d/asterisk restart
bash: /etc/init.d/asterisk: Нет такого файла или каталога
root@rm-09:~# /etc/init.d/asterisk restart
Stopping Asterisk PBX: asterisk.
Starting Asterisk PBX: asterisk.
root@rm-09:~# asterisk -rvvv
Privilege escalation protection disabled!
See https://wiki.asterisk.org/wiki/x/1gKfAQ for more details.
Asterisk 11.7.0~dfsg-lubuntu1, Copyright (C) 1999 - 2013 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.
=====
Connected to Asterisk 11.7.0~dfsg-lubuntu1 currently running on rm-09 (pid = 3148)
rm-09*CLI>

```

Рисунок 25 – Консоль управления Asterisk

8. На РМ запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт UDP 5062 (Рисунок 27), на вкладке «Управление учетными записями SIP» добавить учетную запись с номером РМ (Рисунок 26). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента (Рисунок 28).

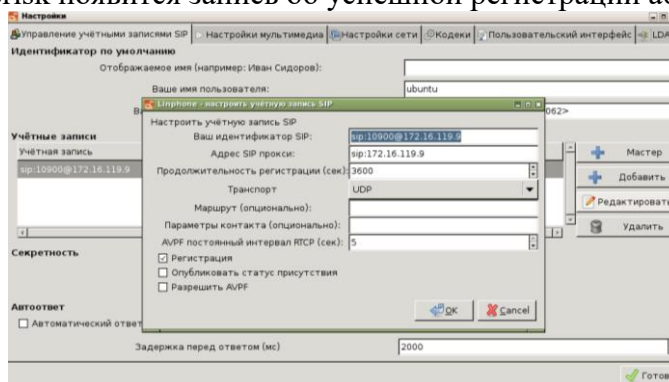


Рисунок 26 – Учетная запись в Linphone

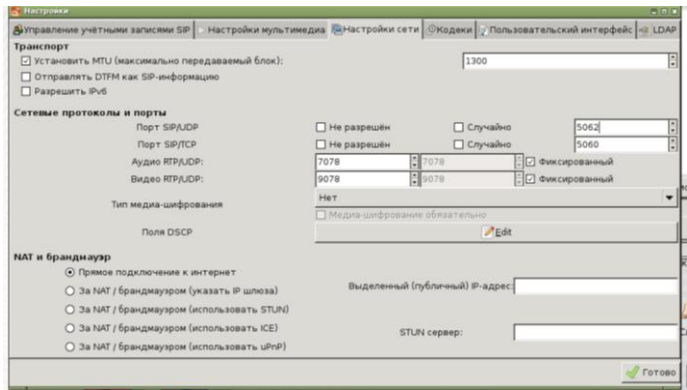


Рисунок 27 – Настройка порта в Linphone

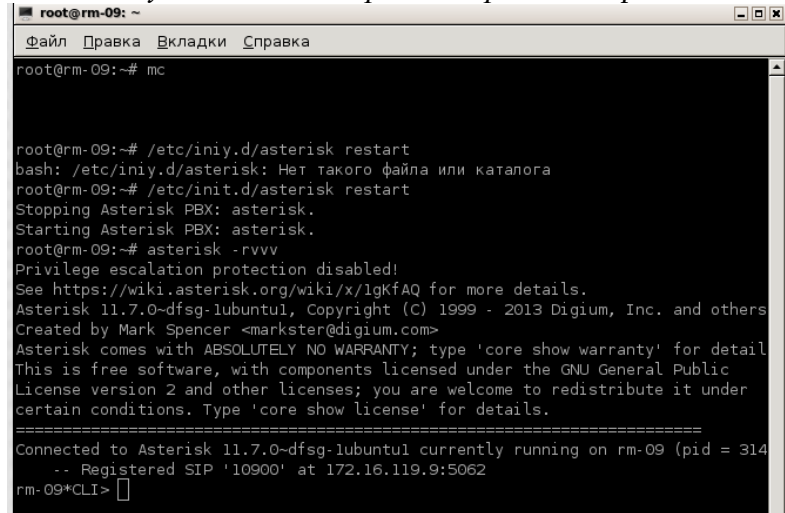


Рисунок 28 – Строка об успешной регистрации абонента Linphone в консоли управления Asterisk

9. Чтобы проверить правильно ли была настроена маршрутизация, осуществляется контрольный вызов на номер 060 (Рисунок 29).

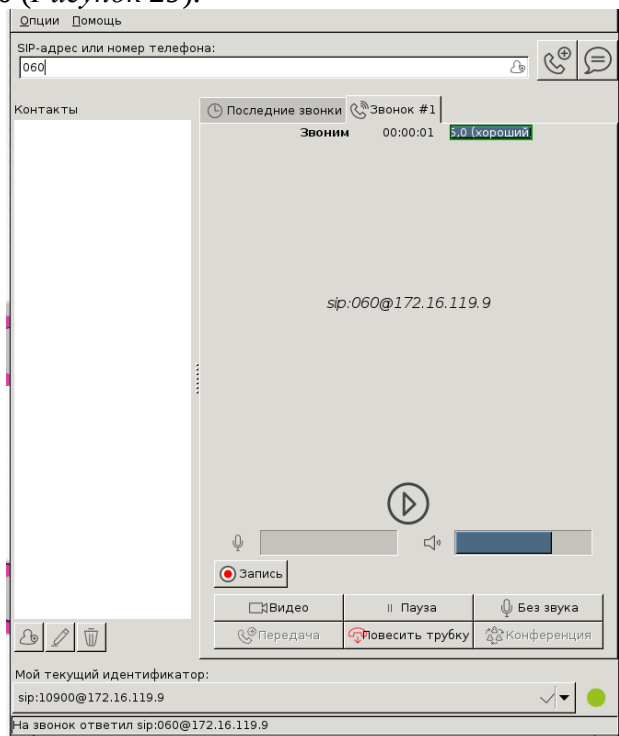


Рисунок 29 – Вызов на номер 060

В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (Рисунок 30, Рисунок 31). Отчет об успешной обработке вызова с пояснениями:
== Using SIP RTP CoS mark 5

```
-- Executing [060@internal:1] Playback("/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja") in new stack
= номер 11000 вызывает 060
-- <SIP/11000-00000000> Playing'/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja.slin' (language 'ru')
= при вызове воспроизводится файл "vremja"
-- Executing [060@internal:2] SayUnixTime("/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja.slin", ",,HM") in new stack
= на номер 060 отправляется запрос точного времени
-- <SIP/11000-00000000> Playing 'digits/14.slin' (language 'ru')
-- <SIP/11000-00000000> Playing 'digits/oh.slin' (language 'ru')
-- <SIP/11000-00000000> Playing 'digits/9.slin' (language 'ru')
= приходит ответ, воспроизводится аудио файл, а именно: Точное время 14:09
-- Executing [060@internal:3] Hangup("/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja.slin", ",,HM") in new stack
= на номер 060 отправляется запрос завершения вызова
== Spawn extension (internal, 060, 3) exited non-zero on 'SIP/11000-00000000'
= завершение вызова
```

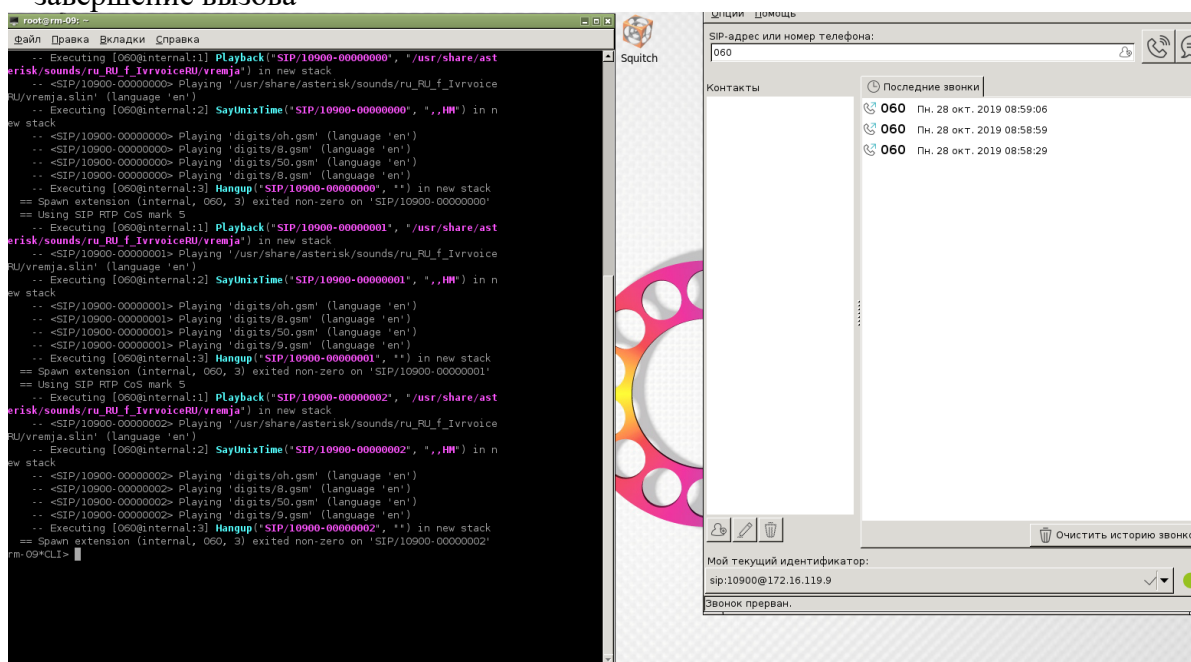


Рисунок 30 – Успешный вызов на номер 060 и сообщения в консоли Asterisk

Таким образом, с помощью этой услуги выяснилось, что точное время в данный момент 14:09. Такое же время показано в правом нижнем углу экрана (Рисунок 32).

```
Connected to Asterisk 11.7.0-dfsg-1ubuntu1 currently running on rm-10 (pid = 2392)
-- Registered SIP '11000' at 172.16.119.10:5062
== Using SIP RTP CoS mark 5
-- Executing [060@internal:1] Playback("/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja") in new stack
-- <SIP/11000-00000000> Playing '/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja.slin' (language 'ru')
-- Executing [060@internal:2] SayUnixTime("/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja.slin", ",,HM") in new stack
-- <SIP/11000-00000000> Playing 'digits/14.slin' (language 'ru')
-- <SIP/11000-00000000> Playing 'digits/oh.slin' (language 'ru')
-- <SIP/11000-00000000> Playing 'digits/9.slin' (language 'ru')
-- Executing [060@internal:3] Hangup("/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja.slin", ",,HM") in new stack
== Spawn extension (internal, 060, 3) exited non-zero on 'SIP/11000-00000000'
rm-10*CLI>
```

Рисунок 31 – Успешная обработка вызова

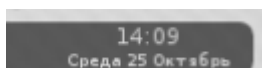


Рисунок 32 – Время в момент совершения вызова

10. Выход из консоли управления Asterisk осуществляется командой `exit`. Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и

маршрутизации, а совпадение времени в правом нижнем углу экрана и времени указанной службой свидетельствует о корректной настройке службы «Точное время».

1.4 Лабораторная работа №3 «Настройка маршрутизации между двумя IP PBX Asterisk»

Предлагаемая нумерация: 1-XX-YY, где XX — номер РМ (01, 02 и т.д.), YY — порядковый номер абонента (00–99). Необходимо изменить настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`.

Будет описана настройка маршрутизации между двумя АТС на РМ №10 и РМ №7.

Каждому программному телефону будет предоставлено два номера.

На (Рисунок 33) изображена схема маршрутизации между двумя АТС, а в таблице 2 приведены рабочие места, на которых установлены АТС, и соответствующие им номера абонентов программных телефонов. Детализированный алгоритм настройки маршрутизации между двумя IP PBX Asterisk в графическом виде представлен на (Рисунок 34).



Рисунок 33 – Схема маршрутизации между двумя АТС

Таблица 2. АТС и соответствующие им номера абонентов программных телефонов

Рабочее место	Программный телефон	Номер программного телефона
РМ №10 (АТС)	Linphone	11000, 11001
РМ №7 (АТС)	Linphone	10700, 10701



Рисунок 34 – Алгоритм настройки маршрутизации между двумя АТС

Алгоритм выполнения работы:

1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).
2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).

3. Для настройки маршрутизации между двумя АТС необходимо изменить настройки, хранящиеся в файлах */etc/asterisk/sip.conf* и */etc/asterisk/extensions.conf*. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

4. Открыть для редактирования файл */etc/asterisk/sip.conf* и добавить 2 абонентов с номерами, соответствующими таблице 2. Пример содержимого файла:

sip.conf (шаблон)

sip.conf (PM №7)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow = all
allow = alaw
allow = ulaw
```

```
[general]
allowguest=no
udpbindaddr=172.16.119.157
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
```

```
[172.16.119.X](!)
type=friend
host=dynamic
context= full
disallow = all
allow = alaw
```

```
[172.16.119.7](!)
type=friend
host=dynamic
context= full
disallow=all
allow=alaw
```

```
[1VV00](172.16.119.X)
[1VV01](172.16.119.X)
```

```
[10700](172.16.119.7)
[10701](172.16.119.7)
```

```
[172.16.119.X](!)
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

```
[172.16.119.10](!)
type=friend
host=172.16.119.160
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

```
[1VV00](172.16.119.X)
[1VV01](172.16.119.X)
```

```
[11000](172.16.119.10)
[11001](172.16.119.10)
```

В шаблоне файла *sip.conf* вместо символов *X* прописывается последнее число IP-адреса РМ; *V* – цифры, обозначающие номера РМ; *Z* – последнее число адреса РМ на сервере Asterisk.

5. В файлы */etc/asterisk/extensions.conf* добавить правила обработки вызовов:

extensions.conf (шаблон):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
```

```

exten => 1VV00,1,Dial(SIP/${EXTEN})
exten => 1VV00,n,Hangup()
[external]
exten => 1VV00,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 1VV00,n,Hangup()
[full]
include => internal
include => external

```

extensions.conf (PM №7):

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 10700,1,Dial(SIP/${EXTEN})
exten => 10700,n,Hangup()
[external]
exten => 11000,1,Dial(SIP/172.16.119.160/${EXTEN})
exten => 11000,n,Hangup()
[full]
include => internal
include => external

```

В шаблоне файла *extensions.conf* вместо символов VV прописываются цифры, обозначающие номера PM; Z – последнее число адреса PM на сервере Asterisk.

Содержание файлов конфигурации подробно описано в приложении 6.

6. Перезапустить процесс asterisk командой */etc/init.d/asterisk restart* (Рисунок 25).

7. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (рис. 4).

8. На PM запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт UDP 5062, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером PM в соответствии с таблицей 2 (приложение 2). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента.

9. Выполнить контрольный межстанционный вызов. В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова. В качестве адресов использовать нумерацию в сети из таблицы 2. При вызове с PM №10 на PM №7 в консоли управления Asterisk на PM №7 отобразиться следующее:

```

== Using SIP RTP CoS mark 5
-- Executing [10700@full:1] Dial("SIP/11000-00000006", "SIP/10700") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/10700
-- SIP/10700-00000007 is ringing
-- SIP/10700-00000007 answered SIP/11000-00000006
-- Remotely bridging SIP/11000-00000006 and SIP/10700-00000007
== Spawn extension (full, 10700, 1) exited non-zero on 'SIP/11000-00000006'

```

10. Выход из консоли управления Asterisk осуществляется командой *exit*.

Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и

маршрутизации между двумя АТС.

1.5 Лабораторная работа №4 «Настройка маршрутизации между двумя IP PBX Asterisk (АТС и УПАТС)»

Нумерация АТС пятизначная, формат 1-XX-YY, где XX — номер РМ (01, 02 и т.д.), YY — порядковый номер абонента (00–99), нумерация УПАТС трехзначная: 1-YY, где YY — порядковый номер абонента (00–99).

В лабораторной работе для настройки маршрутизации необходимо изменить файлы /etc/asterisk/sip.conf и /etc/asterisk/extensions.conf.

В данном разделе будет описана настройка маршрутизации между АТС на РМ №10 и учрежденческо-производственной АТС (УПАТС) на РМ №6.

В данном случае абонент вначале связывается со службой «Технической поддержки», после чего служба перечисляет номера абоненту и связывает абонента с выбранным им номером, в случае если номер не доступен служба прекращает свою работу.

Также стоит отметить, что нумерации АТС и УПАТС отличаются: нумерация АТС пятизначная, тогда как у УПАТС – трехзначная.

На (Рисунок 35) изображена схема маршрутизации между АТС и УПАТС, а в таблице 3 приведены рабочие места, на которых установлены АТС и УПАТС, и соответствующие им номера абонентов программных телефонов. Детализированный алгоритм настройки маршрутизации между двумя IP PBX Asterisk (АТС и УПАТС) в графическом виде представлен на (Рисунок 36).

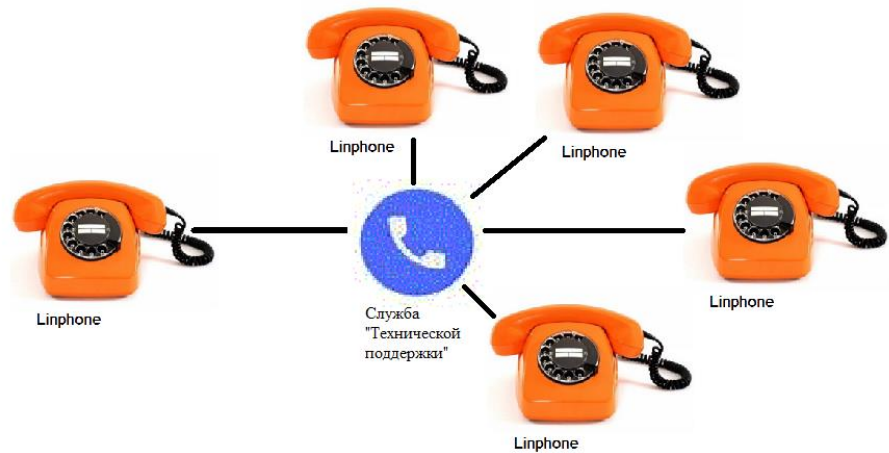


Рисунок 35 – Схема маршрутизации между АТС и УПАТС

Таблица 3. АТС и УПАТС с соответствующие им номера абонентов программных телефонов

Рабочее место	Программный телефон / Служба	Номер
РМ №10 (АТС)	Программный телефон Linphone	11000, 11001
РМ №6 (УПАТС)	Программный телефон Linphone	100, 101, 102, 103
РМ №6 (УПАТС)	Служба «Технической поддержки»	10191



Рисунок 36 – Алгоритм настройки маршрутизации между АТС и УПАТС

Алгоритм выполнения работы:

1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).

2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).

3. Для настройки маршрутизации между АТС и УПАТС необходимо изменить настройки, хранящиеся в файлах */etc/asterisk/sip.conf* и */etc/asterisk/extensions.conf*. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

4. Открыть для редактирования файл */etc/asterisk/sip.conf* и добавить 2 абонентов с номерами, соответствующими таблице 3. Пример содержимого файла:

АТС:

sip.conf (шаблон)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow = all
allow = alaw
allow = ulaw
```

```
[172.16.119.X](!)
type=friend
host=dynamic
context= full
disallow = all
allow = alaw
```

```
[1VV00](172.16.119.X)
[1VV01](172.16.119.X)
```

```
[172.16.119.X](!)
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

```
[Y00](172.16.119.X)
[Y01](172.16.119.X)
```

sip.conf (РМ №10)

```
[general]
allowguest=no
udpbindaddr=172.16.119.160
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
```

```
[172.16.119.10](!)
type=friend
host=dynamic
context= full
disallow=all
allow=alaw
```

```
[11000](172.16.119.10)
[11001](172.16.119.10)
```

```
[172.16.119.6](!)
type=friend
host=172.16.119.156
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

```
[600](172.16.119.6)
[601](172.16.119.6)
```

УПАТС:

sip.conf (шаблон) УПАТС

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

```
[172.16.119.X](!)
type=friend
host=dynamic
context=pbx
disallow=all
allow=alaw
```

```
[Y00](172.16.119.X)
[Y01](172.16.119.X)
[Y02](172.16.119.X)
[Y03](172.16.119.X)
```

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=voice_menu
disallow=all
allow=alaw
```

```
[1VV00](172.16.119.X)
[1VV01](172.16.119.X)
```

sip.conf (PM №6) УПАТС

```
[general]
allowguest=no
udpbindaddr=172.16.119.156
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

```
[172.16.119.6](!)
type=friend
host=dynamic
context=pbx
disallow=all
allow=alaw
```

```
[600](172.16.119.6)
[601](172.16.119.6)
[602](172.16.119.6)
[603](172.16.119.6)
```

```
[172.16.119.10]
type=friend
host=172.16.119.160
port=5060
canreinvite=no
context=voice_menu
disallow=all
allow=alaw
```

```
[11000](172.16.119.10)
[11001](172.16.119.10)
```

В шаблоне файла sip.conf вместо символов X прописывается последнее число IP-адреса РМ; V – цифры, обозначающие номера РМ; Z – последнее число адреса РМ на сервере Asterisk; Y - первая цифра из нумерации РМ в сети (таблица 3).

5. В файлы /etc/asterisk/extensions.conf добавить правила обработки вызовов:

АТС:

extensions.conf (шаблон):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
```

```

exten => 1VV00,1,Dial(SIP/${EXTEN})
exten => 1VV00,n,Hangup()
[external]
exten => 10191,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 10191,n,Hangup()
[full]
include => internal
include => external

```

extensions.conf (PM №10):

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 11000,1,Dial(SIP/${EXTEN})
exten => 11000,n,Hangup()
[external]
exten => 10191,1,Dial(SIP/172.16.119.156/${EXTEN})
exten => 10191,n,Hangup()
[full]
include => internal
include => external

```

extensions.conf (шаблон)УПАТС:

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no

```

[voice_menu]

```

exten => 10191,1,Answer()
exten => 10191,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/thank-you-for-
calling)
exten => 10191,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/to-contact-sales)
exten => 10191,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/najmite-1)
exten => 10191,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/to-contact-tech-
support)
exten => 10191,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/najmite-2)
exten => 10191,n,WaitExten(5)
exten => 1,1,Dial(SIP/101,10)
exten => 1,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ne-otvechaet)
exten => 1,n,Hangup()
exten => 2,1,Dial(SIP/102,10)
exten => 2,n,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ne-otvechaet)

```

```

exten => 2,n,Hangup()
exten => i,1,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/nevernyj-vybor)
exten => i,n,Goto(voice_menu,10191,1)
exten => t,1,Playback (/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/do-svidaniya)
exten => t,n,Hangup()

```

```

[internal]
exten => Y00,1,Dial(SIP/${EXTEN})
exten => Y01,n,Hangup()

```

```

[external]
exten => 1VV00,1,Dial (SIP/172.16.119.Z /${EXTEN:1})
exten => 1VV00,n,Hangup()

```

```

[pbx]
include => internal
include => external

```

В работе в файле *extensions.conf* для УПАТС на РМ №9 были изменены значения шаблона в области [internal] и [external]:

```

[internal]
exten => 600,1,Dial(SIP/${EXTEN})
exten => 601,n,Hangup()

```

```

[external]
exten => 11000,1,Dial(SIP/172.16.119.10/${EXTEN:1})
exten => 11001,n,Hangup()

```

В шаблоне файла *extensions.conf* вместо символов Y прописывается первая цифра из нумерации РМ в сети (таблица 3), Z – последнее число адреса РМ на сервере Asterisk.

Содержание файлов конфигурации подробно описано в приложении 6.

6. Перезапустить процесс Asterisk командой */etc/init.d/asterisk restart* (Рисунок 25).

7. С помощью команды *Asterisk -rvvv* подключиться к консоли управления Asterisk (Рисунок 25).

8. На РМ запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт *UDP 5062*, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером РМ в соответствии с таблицей 3 (приложение 2). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента.

9. Выполнить контрольный межстанционный вызов. В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова. В качестве адресов использовать нумерацию в сети из таблицы 3.

10. Выход из консоли управления Asterisk осуществляется командой *exit*.

В итоге, контекст *[voice_menu]* представляет собой голосовое меню. Вначале команда *Playback()* воспроизводит запись: «Спасибо за ваш звонок. Если вы хотите соединиться с контактными центром, нажмите 1. Если вы хотите соединиться со службой технической поддержки, нажмите 2.»

Затем команда *WaitExten(5)* начинает отсчет времени (5 сек.) данного на ответ. Для ввода цифр во время звонка нажать «Вывод клавиатуры» в меню «Опции».

Если пользователь нажал 1 или 2 и номер 101 или 102, соответственно, зарегистрирован в программном телефоне, то происходит вызов.

Если пользователь нажал 1 или 2, но номер 101 или 102, соответственно, не зарегистрирован в программном телефоне, то воспроизводится голосовое сообщение: «Не отвечает».

Если пользователь нажал другую цифру, помимо 1 или 2, то воспроизводится голосовое сообщение: «Неверный выбор» и команда *Goto()* повторяет все сначала.

Если пользователь не нажал цифру в отведенное ему время, то воспроизводится голосовое сообщение: «До свидания».

Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и маршрутизации между АТС и УПАТС.

1.6 Лабораторная работа №5 «Настройка маршрутизации с установлением видеосвязи»

Будет описана настройка маршрутизации с установлением видеосвязи между двумя АТС на РМ №3 и РМ №4.

IP PBX Asterisk работает с использованием конфигурационных файлов. В данной работе потребуется изменить настройки, хранящиеся в файлах */etc/asterisk/sip.conf* и */etc/asterisk/extensions.conf*. Файл *sip.conf* содержит описание базовых параметров работы протокола SIP, перечень используемых кодеков, учетных записей абонентов и т.д. Файл *extensions.conf* описывает правила обработки вызовов поступающих в систему.

В работе необходимо обеспечить аудио и видео-вызов между двумя пользователями сети в программных телефонах *Liphone* через сервер Asterisk.

В работе участвует группа из двух рабочих мест (РМ). Нумерация абонентов пятизначная (таблица 4). Детализированный алгоритм настройки маршрутизации с установлением видеосвязи в графическом виде представлен на (Рисунок 37).

Таблица 4. Нумерация РМ

№	Номер РМ	Нумерация (общая)	Нумерация
1	РМ №3	1VVXX	10300
2	РМ №4	1VVXX	10400

В общей нумерации вместо символов *X* прописываются номера пользователей, задействованных в работе (например, 01); *V* – цифры, обозначающие номера РМ (например, РМ №4 имеет номер 04).



Рисунок 37 – Алгоритм настройки маршрутизации с установлением видеосвязи

Для поддержки видеовызовов в секцию *[general]* и разделы, описывающие входящие и исходящие вызовы (файл *sip.conf*), необходимо добавить информацию о видеокодеках:

```
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
```

```
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261
```

Алгоритм выполнения работы:

1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).

2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).

3. Для обеспечения аудио и видео вызовов необходимо изменить настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

4. В файл `/etc/asterisk/sip.conf` добавить 2 абонентов с номерами, соответствующими таблице 4. Пример содержимого файлов:

sip.conf (шаблон)

sip.conf (РМ №3)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261
language=ru
```

```
[general]
allowguest=no
udpbindaddr=172.16.119.153
transport=udp
srvlookup=yes
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261
language=ru
```

```
[172.16.119.X](!)
type=friend
host=dynamic
context=full
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261
```

```
[172.16.119.3](!)
type=friend
host=dynamic
context=full
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261
```

[1VV00](172.16.119.X)
[1VV01](172.16.119.X)

[10300](172.16.119.3)
[10301](172.16.119.3)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261

[172.16.119.4]
type=friend
host=172.16.119.154
port=5060
canreinvite=no
context=full
videosupport = yes
disallow = all
allow = alaw
allow = ulaw
allow = gsm
allow = h264
allow = h263
allow = h263p
allow = h261

[1VV00](172.16.119.X)
[1VV01](172.16.119.X)

[10400](172.16.119.4)
[10401](172.16.119.4)

В шаблоне файла *sip.conf* вместо символов X прописывается последнее число IP-адреса PM; V – цифры, обозначающие номера PM; Z – последнее число адреса PM на сервере Asterisk.

5. В файлы */etc/asterisk/extensions.conf* добавить правила обработки вызовов:

extensions.conf (шаблон):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 1VV00,1,Dial(SIP/${EXTEN})
exten => 1VV00,n,Hangup()
[external]
exten => 1VV00,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 1VV00,n,Hangup()
[full]
include => internal
include => external
```

extensions.conf (PM №3):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
```

```

[internal]
exten => 10300,1,Dial(SIP/${EXTEN})
exten => 10300,n,Hangup()
[external]
exten => 10400,1,Dial(SIP/172.16.119.154/${EXTEN})
exten => 10400,n,Hangup()
[full]
include => internal
include => external

```

В шаблоне файла *extensions.conf* вместо символов *VV* прописываются цифры, обозначающие номера РМ; *Z* – последнее число адреса РМ на сервере Asterisk.

Содержание файлов конфигурации подробно описано в приложении 6.

6. Перезапустить процесс *asterisk* командой */etc/init.d/asterisk restart* (Рисунок 25).

7. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (Рисунок 25).

8. На РМ запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт UDP 5062, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером РМ в соответствии с таблицей 4 (приложение 2). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента.

9. Выполнить контрольный межстанционный вызов (Рисунок 38). В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова. В качестве адресов использовать нумерацию в сети из таблицы 4.

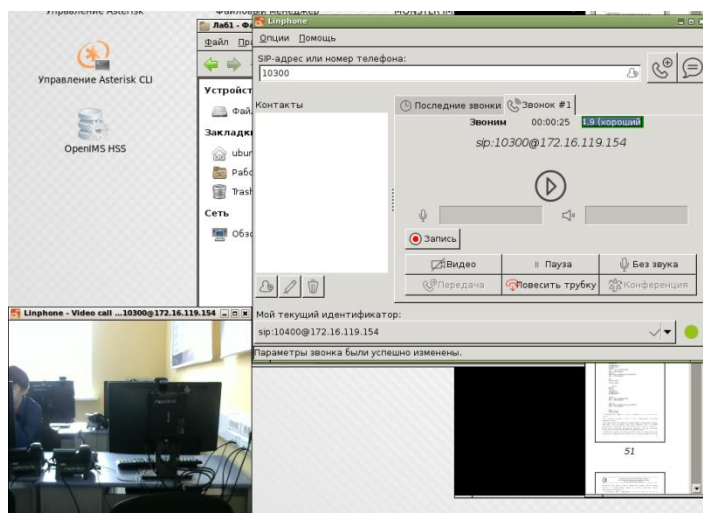


Рисунок 38 – Установка видеовызова

10. Выход из консоли управления Asterisk осуществляется командой *exit*.

Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и маршрутизации с установлением видеосвязи.

1.7 Лабораторная работа №6. «Анализ качества передачи речи по IP-сети»

Будет проанализировано качество передачи речи по IP-сети между двумя АТС на РМ №9 и РМ №2.

Для анализа качества передачи речи по IP-сети необходимо предварительно скопировать из индивидуального каталога учащегося конфигурационные файлы */etc/asterisk/extensions.conf* и

/etc/asterisk/sip.conf, относящиеся к разделу, представленному выше «Настройка маршрутизации между двумя IP PBX Asterisk» и повторить действия, описанные в этом разделе. Детализированный алгоритм анализа качества передачи речи по IP-сети в графическом виде представлен на (Рисунок 39).



Рисунок 39 – Алгоритм анализа качества передачи речи по IP-сети

Алгоритм выполнения работы:

- 1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).
- 2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).
- 3. Для обеспечения аудио вызовов необходимо изменить настройки, хранящиеся в файлах */etc/asterisk/sip.conf* и */etc/asterisk/extensions.conf*. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3). После чего скопировать из индивидуального каталога учащегося конфигурационные файлы */etc/asterisk/extensions.conf* и */etc/asterisk/sip.conf*, относящиеся к разделу, представленному выше «Настройка маршрутизации между двумя IP PBX Asterisk».
- 4. В файле */etc/asterisk/sip.conf* привести к виду (курсивом выделены изменяемые поля):

```
sip.conf (PM №9)
[general]
allowguest=no
udpbindaddr=172.16.119.159
transport=udp
srvlookup=yes
disallow=all
Объявление всех нужных кодеков:
allow=alaw
allow=ulaw
allow=gsm
allow=slin
allow=slin16
allow=speex
allow=speex16
language=ru

[172.16.119.9]
type=friend
```

```
sip.conf (PM №2)
[general]
allowguest=no
udpbindaddr=172.16.119.152
transport=udp
srvlookup=yes
disallow=all
Объявление всех нужных кодеков:
allow=alaw
allow=ulaw
allow=gsm
allow=slin
allow=slin16
allow=speex
allow=speex16
language=ru

[172.16.119.2]
type=friend
```

host=dynamic
context=full
disallow=all
allow=alaw

[10900](172.16.119.9)
[10901](172.16.119.9)

[172.16.119.2]
type=friend
host= 172.16.119.152
port=5062
canreinvite=no
context=full
disallow=all
Кодек, подвергающийся изменению:
allow=gsm

host=dynamic
context=full
disallow=all
allow=alaw

[10200](172.16.119.2)
[10201](172.16.119.2)

[172.16.119.9]
type=friend
host= 172.16.119.159
port=5062
canreinvite=no
context=full
disallow=all
Кодек, подвергающийся изменению:
allow=gsm

В приведенном примере для абонентов IP PBX Asterisk используется кодек *alaw*, а в направлении связи на встречную IP PBX Asterisk - кодек *gsm*. На (Рисунок 40) представлен файл *sip.conf* от РМ №9.

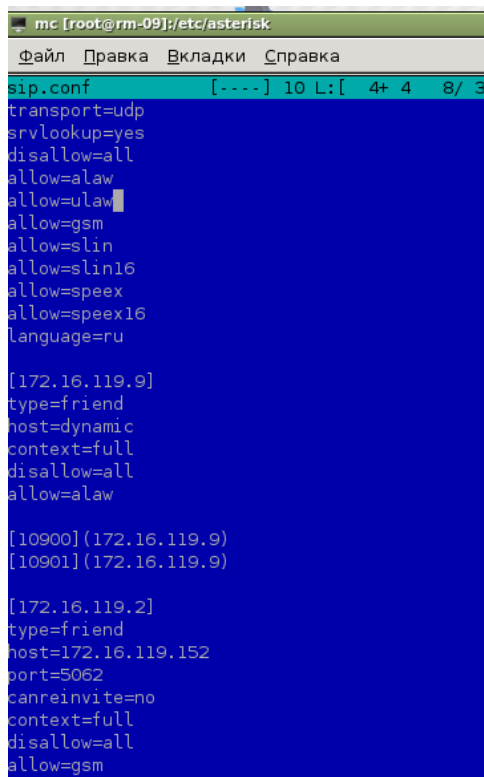


Рисунок 40 – Файл *sip.conf* РМ №9

5. Перезапустить процесс *asterisk* командой */etc/init.d/asterisk restart* (рис. 4).

6. В консоли управления Asterisk, запуск которой осуществляется командой *asterisk -rvvv* (Рисунок 25). Дать команду *core show translation* для отображения списка установленных кодеков и времени преобразования из одного кодека в другой. Работоспособность команды представлена на (Рисунок 41).

```
rm-09*CLI> core show translation
```

Translation times between formats (in microseconds) for one second of data

Source Format (Rows) Destination Format (Columns)

	gsm	ulaw	alaw	g726	adpcm	slin	lpc10	speex	speex16	g726aal2	g722	slin16	testlaw	speex32	slin12	slin24	slin32	slin44	slin48	slin96	slin192
gsm	-	15000	15000	15000	15000	9000	15000	15000	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
ulaw	15000	-	9150	15000	15000	9000	15000	15000	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
alaw	15000	9150	-	15000	15000	9000	15000	15000	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
g726	15000	15000	15000	-	15000	9000	15000	15000	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
adpcm	15000	15000	15000	15000	-	9000	15000	15000	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
slin	6000	6000	6000	6000	6000	-	6000	6000	14000	6000	8250	8000	6000	14000	8000	8000	8000	8000	8000	8000	8000
lpc10	15000	15000	15000	15000	15000	9000	-	15000	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
speex	15000	15000	15000	15000	15000	9000	15000	-	23000	15000	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
speex16	23500	23500	23500	23500	23500	17500	23500	23500	-	23500	15000	9000	23500	23000	17500	17000	17000	17000	17000	17000	17000
g726aal2	15000	15000	15000	15000	15000	9000	15000	15000	23000	-	17250	17000	15000	23000	17000	17000	17000	17000	17000	17000	17000
g722	15600	15600	15600	15600	15600	9600	15600	15600	15000	15600	-	9000	15600	23000	17500	17000	17000	17000	17000	17000	17000
slin16	14500	14500	14500	14500	14500	8500	14500	14500	6000	14500	6000	-	14500	14000	8500	8000	8000	8000	8000	8000	8000
testlaw	15000	15000	15000	15000	15000	9000	15000	15000	23000	15000	17250	17000	-	23000	17000	17000	17000	17000	17000	17000	17000
speex32	23500	23500	23500	23500	23500	17500	23500	23500	23500	23500	23500	17500	23500	-	17500	17500	9000	17000	17000	17000	17000
slin12	14500	14500	14500	14500	14500	8500	14500	14500	14000	14500	14000	8000	14500	14000	-	8000	8000	8000	8000	8000	8000
slin24	14500	14500	14500	14500	14500	8500	14500	14500	14500	14500	14500	8500	14500	14000	8500	-	8000	8000	8000	8000	8000
slin32	14500	14500	14500	14500	14500	8500	14500	14500	14500	14500	14500	8500	14500	6000	8500	8500	-	8000	8000	8000	8000
slin44	14500	14500	14500	14500	14500	8500	14500	14500	14500	14500	14500	8500	14500	14500	8500	8500	8500	-	8000	8000	8000
slin48	14500	14500	14500	14500	14500	8500	14500	14500	14500	14500	14500	8500	14500	14500	8500	8500	8500	8500	-	8000	8000
slin96	14500	14500	14500	14500	14500	8500	14500	14500	14500	14500	14500	8500	14500	14500	8500	8500	8500	8500	8500	-	8000
slin192	14500	14500	14500	14500	14500	8500	14500	14500	14500	14500	14500	8500	14500	14500	8500	8500	8500	8500	8500	8500	-

```
rm-09*CLI>
```

Рисунок 41 – Команда core show translation на РМ №9.

7. На РМ запустить локальный Wireshark (приложение 3) и произвести захват трафика протокола RTP. Изменяя параметр allow="кодек" в секции, описывающий встречный Asterisk (Рисунок 42), и производя контрольные вызовы, составлена таблица занимаемой полосы каждым из кодеков и поставлена субъективная оценка качества передаваемой речи (оценка зависит от занимаемой полосы). После внесения изменений в файл конфигурации и его сохранения необходимо перезапустить процесс Asterisk.

```
mc [root@rm-09]:/etc/asterisk
Файл Правка Вкладки
sip.conf [---]
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
allow=gsm
allow=slin
allow=slin16
allow=speex
allow=speex16
language=ru

[172.16.119.9]
type=friend
host=dynamic
context=full
disallow=all
allow=alaw

[10900] (172.16.119.9)
[10901] (172.16.119.9)

[172.16.119.2]
type=friend
host=172.16.119.152
port=5062
canreinvite=no
context=full
disallow=all
allow=gsm
```

Рисунок 42 – Изменение параметра allow

Для определения полосы в Wireshark требуется задать соответствующие фильтры, например, ip.src==172.16.119.159 &&ip.dst==172.16.119.152&&rtp (Рисунок 43) и выбрать пункт меню Statistics — Protocol Hierarchy Statistics.

Данные с поля Bits/s строки Real-Time Transport Protocol записаны в таблицу 5.

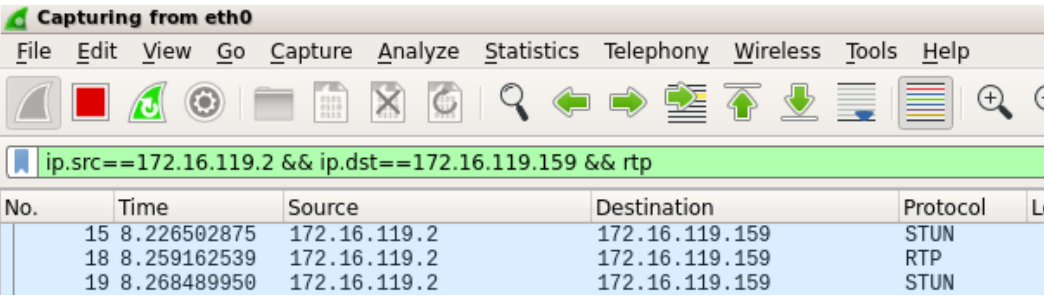


Рисунок 43 – Задать соответствующие фильтры.

Таблица 5. Субъективная оценка качества передачи данных с использованием разных кодеков

№	Кодек	Занимаемая полоса, KB/s	Субъективная оценка качества	Примечание
1	Spreex	36	4	Слабая скорость передачи
2	Spreex16	45	4	Приемлемая скорость передачи
3	A-law	85	5	Один из самых быстрых кодеков
4	U-law	85	5	Один из самых быстрых кодеков

Отчеты всех захватов приведены на (Рисунок 44, Рисунок 45, Рисунок 46, Рисунок 47).

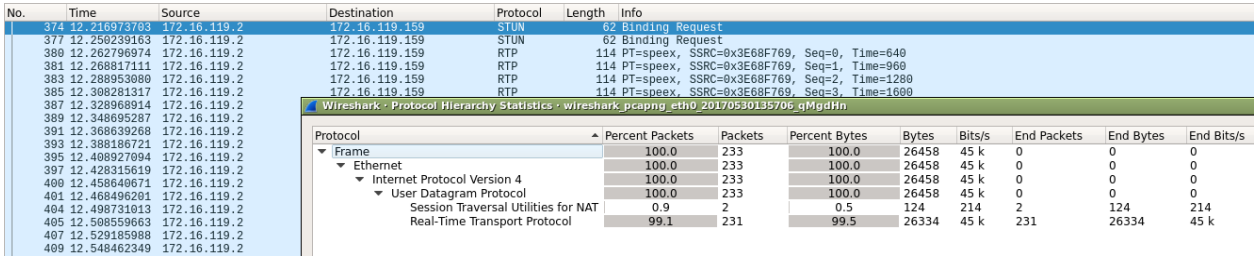


Рисунок 44 – Захват кодека Spreex

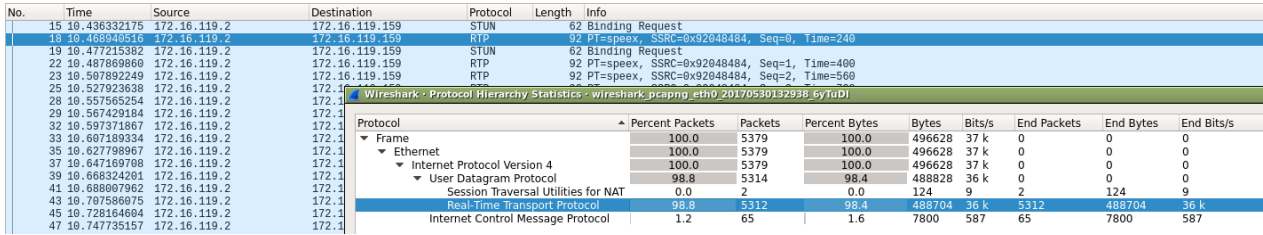


Рисунок 45 – Захват кодека Spreex16

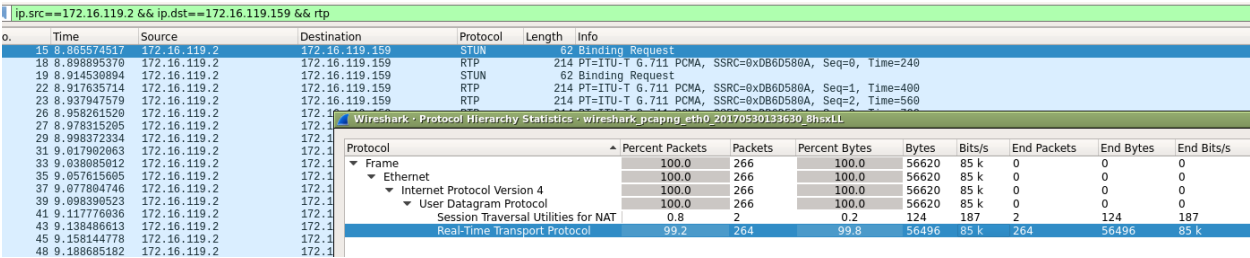


Рисунок 46 – Захват кодека A-law

ip.src==172.16.119.2 && ip.dst==172.16.119.159 && rtp						
No.	Time	Source	Destination	Protocol	Length	Info
15	8.226592875	172.16.119.2	172.16.119.159	STUN	62	Binding Request
18	8.259162539	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=0, Time=240
19	8.268489950	172.16.119.2	172.16.119.159	STUN	62	Binding Request
22	8.278380508	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=1, Time=400
23	8.298499929	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=2, Time=560
25	8.318723594	172.16.119.2	172.16.119.159	STUN	62	Binding Request
27	8.339167207	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=3, Time=720
29	8.358177744	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=4, Time=880
31	8.378228513	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=5, Time=1040
33	8.398149214	172.16.119.2	172.16.119.159	STUN	62	Binding Request
35	8.418338619	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=6, Time=1200
37	8.437995248	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=7, Time=1360
40	8.468271975	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=8, Time=1520
41	8.478639638	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=9, Time=1680
43	8.498549483	172.16.119.2	172.16.119.159	STUN	62	Binding Request
45	8.518299712	172.16.119.2	172.16.119.159	RTP	214	PT=ITU-T 6.711 PCMU, SSRC=0xBECBC64E, Seq=10, Time=1840

Wireshark - Protocol Hierarchy Statistics - wireshark.pcapng.eth0.20170530134137.uIWQKZ

Protocol	% Percent Packets	Packets	Percent Bytes	Bytes	Bits/s	End Packets	End Bytes	End Bits/s
▼ Frame	100.0	548	100.0	116968	85 k	0	0	0
▼ Ethernet	100.0	548	100.0	116968	85 k	0	0	0
▼ Internet Protocol Version 4	100.0	548	100.0	116968	85 k	0	0	0
▼ User Datagram Protocol	100.0	548	100.0	116968	85 k	0	0	0
Session Traversal Utilities for NAT	0.4	2	0.1	124	90	2	124	90
Real-time Transport Protocol	99.6	546	99.9	116844	85 k	546	116844	85 k

Рисунок 47 – Захват кодека U-law

8. Выход из консоли управления Asterisk осуществляется командой *exit*.

Таким образом, из таблицы 5 определены кодеки, с наивысшей скоростью передачи данных: *A-law* и *U-law*.

1.8 Лабораторная работа №7. «Построение сети связи. Районированная ГТС без узлообразованния»

Будет описано построение сети связи: районированная ГТС без узлообразованния на РМ №1-5.

Районированная ГТС – это городская АТС, все районированные АТС (РАТС) которой соединены по принципу «каждый с каждым».

В работе необходимо построить на полигоне СОТСБИ-NGN сеть связи в соответствии со схемой, заданной на (Рисунок 48).

Каждое рабочее место представляет собой один из узлов на схеме и настраивает необходимые для корректной работы сети функции.

В работе участвует группа из пяти рабочих мест. Нумерация абонентов шестизначная (таблица 6). Схема сети представлена на (Рисунок 48). Детализированный алгоритм построения районированной ГТС без узлообразованния в графическом виде представлен на (Рисунок 49).

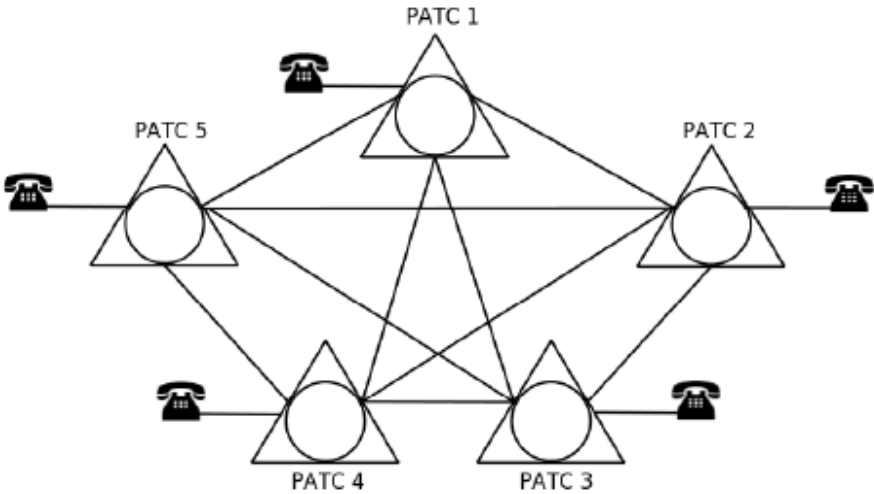


Рисунок 48 –Районированная ГТС без узлообразованния

Таблица 6. Нумерация сети

№	Номер АТС	Нумерация (общая)	Нумерация	РМ, использующиеся в работе
1	РАТС №1	1XXXXXX	100000	РМ №1
2	РАТС №2	2XXXXXX	200000	РМ №2
3	РАТС №3	3XXXXXX	300000	РМ №3
4	РАТС №4	4XXXXXX	400000	РМ №4
5	РАТС №5	5XXXXXX	500000	РМ №5



Рисунок 49 –Алгоритм построения районированной ГТС без узообразования

Алгоритм выполнения работы:

1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).

2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).

3. Для построения сети связи необходимо изменить настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

4. В файл `/etc/asterisk/sip.conf` добавить 5 абонентов с номерами, соответствующими таблице 6. Пример содержимого файлов:

sip.conf (шаблон)

sip.conf (PATC №1)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

```
[general]
allowguest=no
udpbindaddr=172.16.119.151
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

`[172.16.119.X](!)`

`[172.16.119.1](!)`

```
type=friend
host=dynamic
context=full
disallow=all
allow=alaw
```

```
type=friend
host=dynamic
context=full
disallow=all
allow=alaw
```

```
[Y00000](172.16.119.X)
[Y00001](172.16.119.X)
```

```
[100000](172.16.119.1)
[100001](172.16.119.1)
```

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
```

```
[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
```

context=full
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

context=full
disallow=all
allow=alaw

[200000](172.16.119.2)
[200001](172.16.119.2)

[172.16.119.3]
type=friend
host=172.16.119.153
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[300000](172.16.119.3)
[300001](172.16.119.3)

[172.16.119.4]
type=friend
host=172.16.119.154
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[400000](172.16.119.4)
[400001](172.16.119.4)

[172.16.119.5]
type=friend
host=172.16.119.155
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[500000](172.16.119.5)
[500001](172.16.119.5)

В шаблоне файла *sip.conf* вместо символов *X* прописывается последнее число IP-адреса РМ, *Y* - первая цифра из нумерации РМ в сети (таблица 6), *Z* – последнее число адреса РМ на сервере Asterisk.

5. В файлы */etc/asterisk/extensions.conf* добавить правила обработки вызовов:

extensions.conf (шаблон):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => Y00000,1,Dial(SIP/${EXTEN})
exten => Y00000,n,Hangup()
[external]
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => Y00000,n,Hangup()
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => Y00000,n,Hangup()
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => Y00000,n,Hangup()
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => Y00000,n,Hangup()
[full]
include => internal
include => external
```

extensions.conf (PATC №1):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 100000,1,Dial(SIP/${EXTEN})
exten => 100000,n,Hangup()
[external]
exten => 200000,1,Dial(SIP/172.16.119.152/${EXTEN})
exten => 200000,n,Hangup()
exten => 300000,1,Dial(SIP/172.16.119.153/${EXTEN})
exten => 300000,n,Hangup()
exten => 400000,1,Dial(SIP/172.16.119.154/${EXTEN})
exten => 400000,n,Hangup()
exten => 500000,1,Dial(SIP/172.16.119.155/${EXTEN})
exten => 500000,n,Hangup()
[full]
include => internal
include => external
```

В шаблоне файла *extensions.conf* вместо символов Y прописывается первая цифра из нумерации РМ в сети (таблица 6), Z – последнее число адреса РМ на сервере Asterisk.

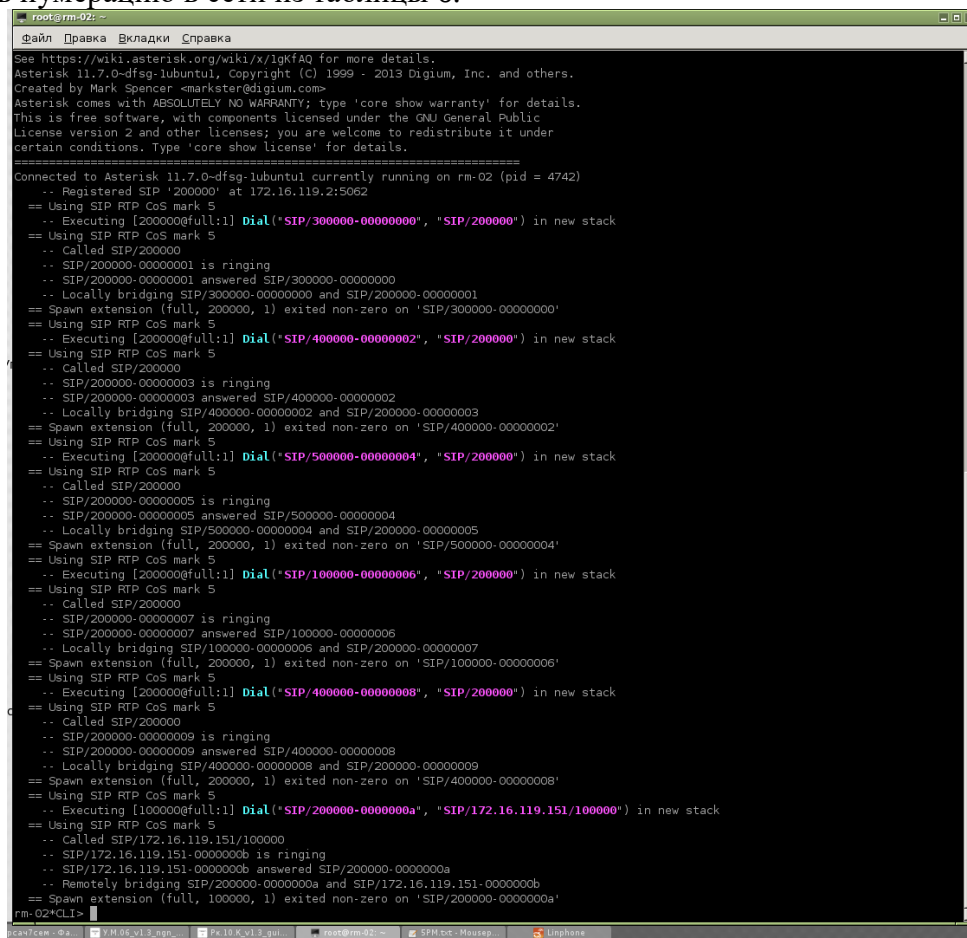
Содержание файлов конфигурации подробно описано в приложении 6.

6. Перезапустить процесс *asterisk* командой */etc/init.d/asterisk restart* (Рисунок 25).

7. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (Рисунок 25).

8. На РМ запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт *UDP 5062*, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером РМ в соответствии с таблицей 6 (приложение 2). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента.

Выполнить контрольный межстанционный вызов. В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (Рисунок 50). В качестве адресов использовать нумерацию в сети из таблицы 6.



```
root@rm-02: ~
See https://wiki.asterisk.org/wiki/x/1gkFAQ for more details.
Asterisk 11.7.0-dfsg-lubuntu, Copyright (C) 1999 - 2013 Digium, Inc. and others.
Created by Mark Spencer <markster@digium.com>
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.
This is free software, with components licensed under the GNU General Public
License version 2 and other licenses; you are welcome to redistribute it under
certain conditions. Type 'core show license' for details.

=====
Connected to Asterisk 11.7.0-dfsg-lubuntu currently running on rm-02 (pid = 4742)
-- Registered SIP '200000' at 172.16.119.2:5062
== Using SIP RTP CoS mark 5
-- Executing [200000@full:1] Dial(*SIP/300000-00000000, "SIP/200000") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/200000
-- SIP/200000-00000001 is ringing
-- SIP/200000-00000001 answered SIP/300000-00000000
-- Locally bridging SIP/300000-00000000 and SIP/200000-00000001
== Spawn extension (full, 200000, 1) exited non-zero on 'SIP/300000-00000000'
== Using SIP RTP CoS mark 5
-- Executing [200000@full:1] Dial(*SIP/400000-00000002, "SIP/200000") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/200000
-- SIP/200000-00000003 is ringing
-- SIP/200000-00000003 answered SIP/400000-00000002
-- Locally bridging SIP/400000-00000002 and SIP/200000-00000003
== Spawn extension (full, 200000, 1) exited non-zero on 'SIP/400000-00000002'
== Using SIP RTP CoS mark 5
-- Executing [200000@full:1] Dial(*SIP/500000-00000004, "SIP/200000") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/200000
-- SIP/200000-00000005 is ringing
-- SIP/200000-00000005 answered SIP/500000-00000004
-- Locally bridging SIP/500000-00000004 and SIP/200000-00000005
== Spawn extension (full, 200000, 1) exited non-zero on 'SIP/500000-00000004'
== Using SIP RTP CoS mark 5
-- Executing [200000@full:1] Dial(*SIP/100000-00000006, "SIP/200000") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/200000
-- SIP/200000-00000007 is ringing
-- SIP/200000-00000007 answered SIP/100000-00000006
-- Locally bridging SIP/100000-00000006 and SIP/200000-00000007
== Spawn extension (full, 200000, 1) exited non-zero on 'SIP/100000-00000006'
== Using SIP RTP CoS mark 5
-- Executing [200000@full:1] Dial(*SIP/400000-00000008, "SIP/200000") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/200000
-- SIP/200000-00000009 is ringing
-- SIP/200000-00000009 answered SIP/400000-00000008
-- Locally bridging SIP/400000-00000008 and SIP/200000-00000009
== Spawn extension (full, 200000, 1) exited non-zero on 'SIP/400000-00000008'
== Using SIP RTP CoS mark 5
-- Executing [100000@full:1] Dial(*SIP/200000-0000000a, "SIP/172.16.119.151/100000") in new stack
== Using SIP RTP CoS mark 5
-- Called SIP/172.16.119.151/100000
-- SIP/172.16.119.151-0000000b is ringing
-- SIP/172.16.119.151-0000000b answered SIP/200000-0000000a
-- Remotely bridging SIP/200000-0000000a and SIP/172.16.119.151-0000000b
== Spawn extension (full, 100000, 1) exited non-zero on 'SIP/200000-0000000a'
rm-02*CLI>
```

Рисунок 50 – Сообщения о ходе обработки вызовов в сети

10. Выход из консоли управления Asterisk осуществляется командой *exit*.

Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и районированной ГТС без узлообразования.

1.9 Лабораторная работа №8. «Построение сети связи. Районированная ГТС без узлообразования с узлом УСС»

В работе необходимо построить на полигоне СОТСБИ-NGN сеть связи в соответствии со схемой, заданной на (Рисунок 51). Схема включает в себя 3 РАТС, узел спецслужб (УСС) и учрежденческо-производственную АТС (УПАТС).

Каждое рабочее место представляет собой один из узлов на схеме и настраивает необходимые для корректной работы сети функции.

В работе участвует группа из пяти рабочих мест. Нумерация абонентов РАТС шестизнач-

ная, УСС и УПАТС трехзначная (таблица 7). Схема сети представлена на (Рисунок 51). Детализированный алгоритм построения районированной ГТС без узлообразования с узлом УСС в графическом виде представлен на (Рисунок 52).

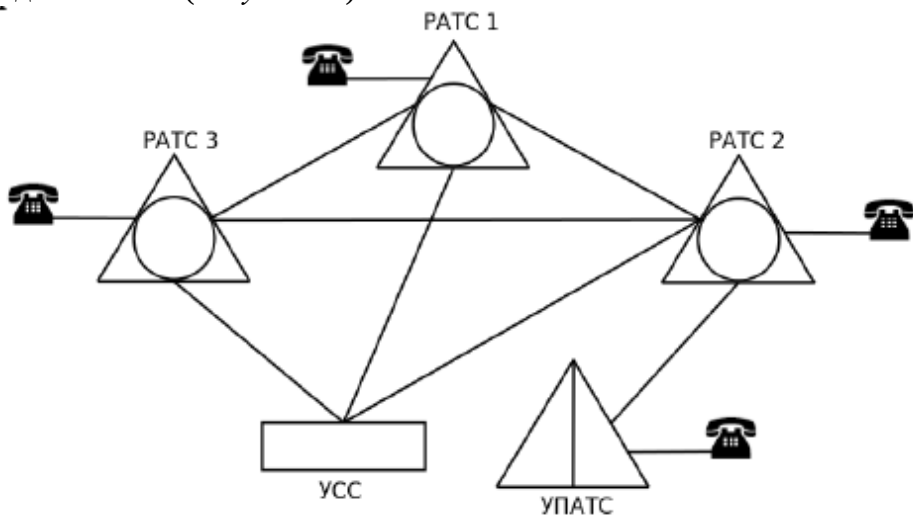


Рисунок 51 – Районированная ГТС без узлообразования с узлом УСС

Таблица 7. Нумерация сети с узлом УСС

№	Номер АТС	Нумерация (общая)	Нумерация	РМ, использующиеся в работе
1	ПАТС №1	1XXXXXX	100000	РМ №1
2	ПАТС №2	2XXXXXX	200000	РМ №2
3	ПАТС №3	3XXXXXX	300000	РМ №3
4	УСС	0XX и 112	060, 02, 03 и 112	РМ №4
5	УПАТС	9XX	900, 901	РМ №9

Для настройки УСС необходимо определить на нем функции служб, прописав адреса соответствующих звуковых файлов:

- 02 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_02
- 03 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_03
- 060 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja
- 112 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_112

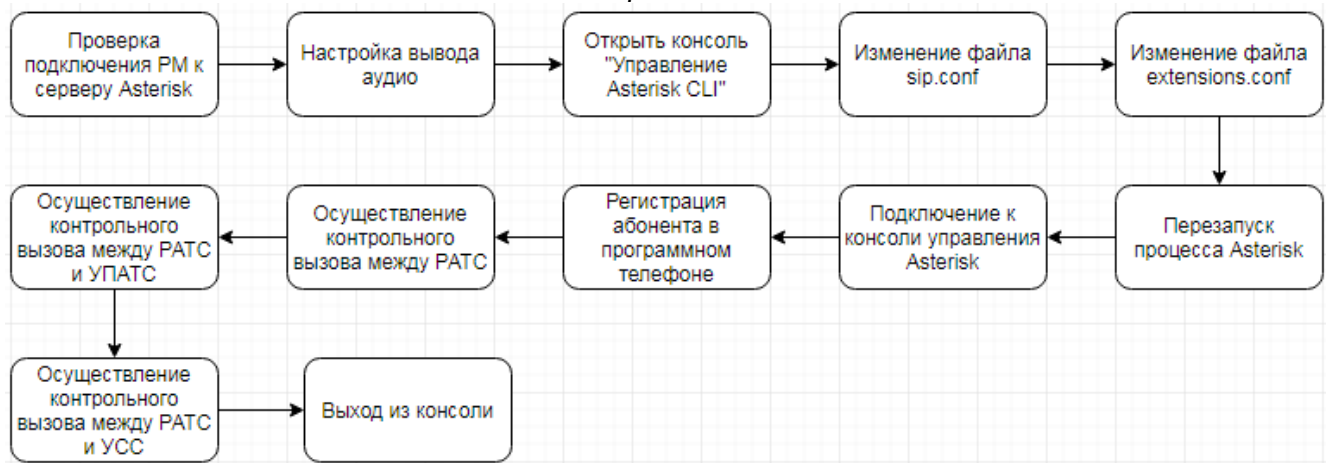


Рисунок 52 – Алгоритм построения районированной ГТС без узлообразования с узлом УСС

Алгоритм выполнения работы:

1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программах Twinkle и Linphone (приложение 4).

2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).

3. Для построения сети связи необходимо изменить настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

4. В файл `/etc/asterisk/sip.conf` добавить 5 абонентов с номерами, соответствующими таблице 7. Пример содержимого файлов:

PATC №1-3:

sip.conf (шаблон)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

`[172.16.119.X](!)`

```
type=friend
host=dynamic
context=full
disallow=all
allow=alaw
```

`[Y00000](172.16.119.X)`

`[Y00001](172.16.119.X)`

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

`[Y00000](172.16.119.X)`

`[Y00001](172.16.119.X)`

`[172.16.119.X]`

sip.conf (PATC №1)

```
[general]
allowguest=no
udpbindaddr=172.16.119.151
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

`[172.16.119.1](!)`

```
type=friend
host=dynamic
context=full
disallow=all
allow=alaw
```

`[100000](172.16.119.1)`

`[100001](172.16.119.1)`

```
[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

`[200000](172.16.119.2)`

`[200001](172.16.119.2)`

`[172.16.119.3]`

*type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw*

*[Y00000](172.16.119.X)
[Y00001](172.16.119.X)*

*[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw*

*[Y00000](172.16.119.X)
[Y00001](172.16.119.X)*

*[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw*

*[Y00](172.16.119.X)
[Y01](172.16.119.X)*

YCC:

sip.conf (шаблон) YCC

*[general]
allowguest=no
udpbindingaddr=172.16.119.Z
transport=udp
srlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru*

*type=friend
host=172.16.119.153
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw*

*[300000](172.16.119.3)
[300001](172.16.119.3)*

*[172.16.119.4]
type=friend
host=172.16.119.154
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw*

*[400000](172.16.119.4)
[400001](172.16.119.4)*

*[172.16.119.5]
type=friend
host=172.16.119.155
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw*

*[500](172.16.119.5)
[501](172.16.119.5)*

sip.conf (PM №4) YCC

*[general]
allowguest=no
udpbindingaddr=172.16.119.154
transport=udp
srlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru*

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

[172.16.119.1]
type=friend
host=172.16.119.151
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw

[100000](172.16.119.1)
[100001](172.16.119.1)

[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw

[200000](172.16.119.2)
[200001](172.16.119.2)

[172.16.119.3]
type=friend
host=172.16.119.153
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw

[300000](172.16.119.3)
[300001](172.16.119.3)

УПАТС:

sip.conf (шаблон) УПАТС
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru

sip.conf (PM №9) УПАТС
[general]
allowguest=no
udpbindaddr=172.16.119.159
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru

```
[172.16.119.X](!)
type=friend
host=dynamic
context=pbx
disallow=all
allow=alaw
```

```
[172.16.119.9](!)
type=friend
host=dynamic
context=pbx
disallow=all
allow=alaw
```

```
[500](172.16.119.X)
[501](172.16.119.X)
[502](172.16.119.X)
[503](172.16.119.X)
```

```
[500](172.16.119.9)
[501](172.16.119.9)
[502](172.16.119.9)
[503](172.16.119.9)
```

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=voice_menu
disallow=all
allow=alaw
```

```
[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=voice_menu
disallow=all
allow=alaw
```

```
[Y00000](172.16.119.X)
[Y00001](172.16.119.X)
```

```
[200000](172.16.119.2)
[200001](172.16.119.2)
```

В шаблоне файла *sip.conf* вместо символов *X* прописывается последнее число IP-адреса РМ, *Y* - первая цифра из нумерации РМ в сети (таблица 7), *Z* – последнее число адреса РМ на сервере Asterisk.

5. В файлы */etc/asterisk/extensions.conf* добавить правила обработки вызовов:
extensions.conf (шаблон) РАТС №1-3:

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => X00000,1,Dial(SIP/${EXTEN})
exten => X00000,n,Hangup()
[external]
exten => X00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => X00000,n,Hangup()
exten => X00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => X00000,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 02,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 03,n,Hangup()
```

```

exten => 060,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 060,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 112,n,Hangup()
exten => 399900,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 399900,n,Hangup()
[full]
include => internal
include => external

```

extensions.conf (PATC №1):

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 100000,1,Dial(SIP/${EXTEN})
exten => 100000,n,Hangup()
[external]
exten => 200000,1,Dial(SIP/172.16.119.2/${EXTEN})
exten => 200000,n,Hangup()
exten => 300000,1,Dial(SIP/172.16.119.3/${EXTEN})
exten => 300000,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.4/${EXTEN})
exten => 02,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.4/${EXTEN})
exten => 03,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119.4/${EXTEN})
exten => 060,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.4/${EXTEN})
exten => 112,n,Hangup()
exten => 399900,1,Dial(SIP/172.16.119.9/${EXTEN})
exten => 399900,n,Hangup()
[full]
include => internal
include => external

```

extensions.conf (YCC):

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 060,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja)
exten => 060,n,SayUnixTime(,HM)

```

```

exten => 060,n,Hangup()
exten => 02,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_02)
exten => 02,n,Hangup()
exten => 03,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_03)
exten => 03,n,Hangup()
exten => 112,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_112)
exten => 112,n,Hangup()

```

extensions.conf (шаблон)УПАТС:

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[voice_menu]
exten => 399900,1,Answer()
exten => 399900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/thank-you-for-calling)
exten => 399900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/to-contact-sales)
exten => 399900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/najmite-1)
exten => 399900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/to-contact-tech-support)
exten => 399900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/najmite-2)
exten => 399900,n,WaitExten(5)
exten => 1,1,Dial(SIP/201,10)
exten => 1,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ne-otvechaet)
exten => 1,n,Hangup()
exten => 2,1,Dial(SIP/202,10)
exten => 2,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ne-otvechaet)
exten => 2,n,Hangup()
exten => i,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/nevernyj-vybor)
exten => i,n,Goto(voice_menu,399900,1)
exten => t,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/do-svidaniya)
exten => t,n,Hangup()

```

```

[internal]
exten => Y00,1,Dial(SIP/${EXTEN})
exten => Y00,n,Hangup()

```

```

[external]
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
exten => Y00000,n,Hangup()

```

```

[pbx]
include => internal
include => external

```

В работе в файле extensions.conf для УПАТС на РМ №9 были изменены значения шаблона в областях [internal] и [external]:

```
[internal]
```

```
exten => 900,1,Dial(SIP/${EXTEN})
exten => 900,n,Hangup()
[external]
exten => 200000,1,Dial(SIP/172.16.119.2/${EXTEN:1})
exten => 200000,n,Hangup()
```

В шаблоне файла extensions.conf вместо символов Y прописывается первая цифра из нумерации РМ в сети (таблица 7), Z – последнее число адреса РМ на сервере Asterisk.

Содержание файлов конфигурации подробно описано в приложении 6.

6. Перезапустить процесс asterisk командой /etc/init.d/asterisk restart (Рисунок 25).

7. С помощью команды asterisk -rvvv подключиться к консоли управления Asterisk (Рисунок 25).

8. На РМ №1-3,5 запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт UDP 5062, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером РМ в соответствии с таблицей 7 (приложение 2). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента.

9. Выполнить контрольный межстанционный вызов между РАТС №1-3. В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (Рисунок 53). В качестве адресов использовать нумерацию в сети из таблицы 7.

10. Выполнить контрольный межстанционный вызов между РАТС 2 и УПАТС. Для этого использовать в качестве адреса «399900». При вызове прослушать информацию о сотрудниках и после её окончания нажать 1 или 2 для соединения с оператором. Для ввода цифр во время звонка нажать «Вывод клавиатуры» в меню «Опции». В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (Рисунок 53).

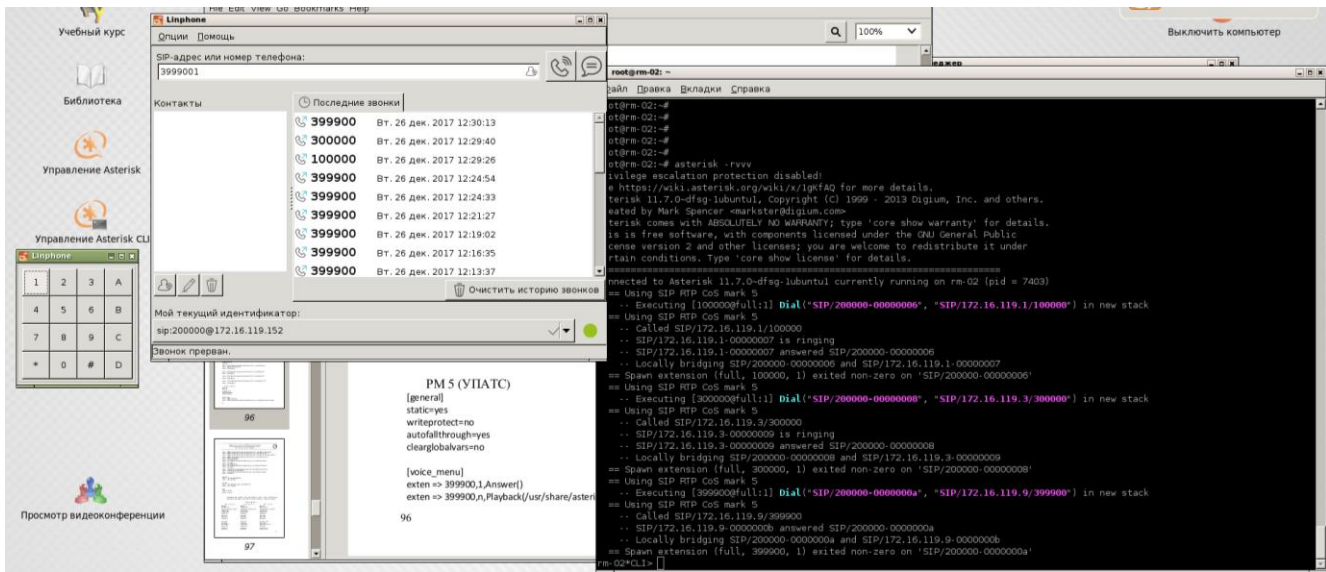
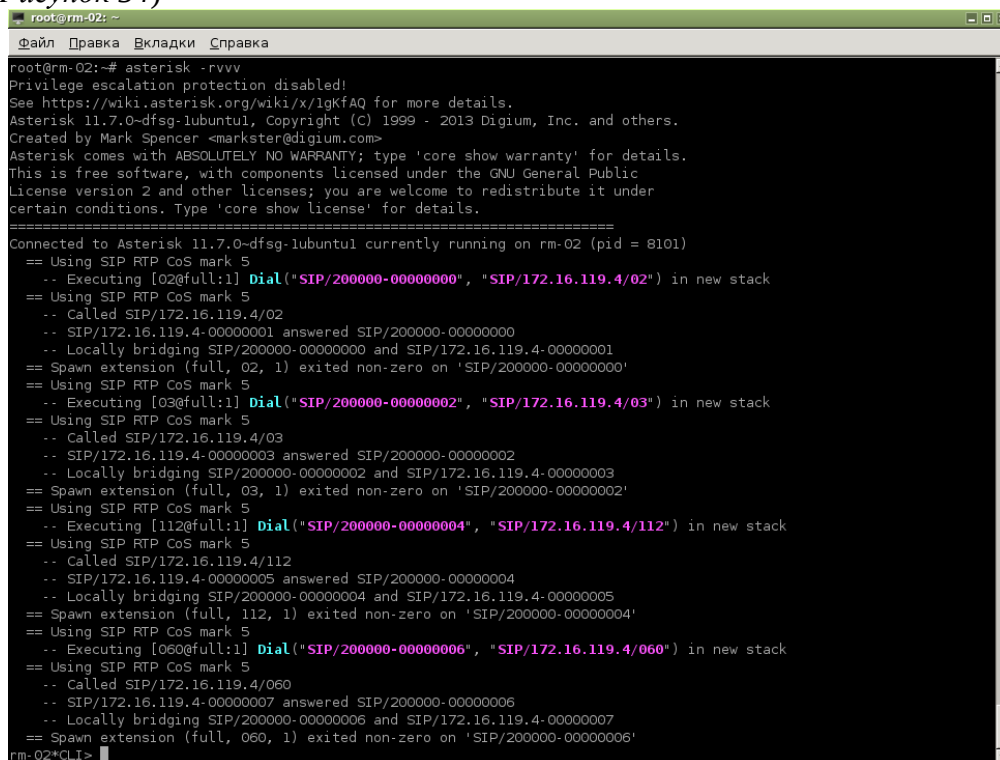


Рисунок 53 – Сообщения о ходе обработки вызовов, при обращении к узлу УПАТС и РАТС №1,3

11. Выполнить контрольный межстанционный вызов между РАТС 1-3 и УСС. Для этого использовать в качестве адреса нумерацию подключенных служб (таблица 7). При вызове данных служб будет слышен:

- «060» - говорится, женским голосом, точное время, установленное в системе;
- «02» - фраза «полиция», сказанная мужским голосом;
- «03» - фраза «скорая медицинская помощь», сказанная женским голосом;
- «112» - фраза «экстренные оперативные службы», сказанная мужским голосом.

В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (*Рисунок 54*)



```
root@rm-02: ~  
Файл Правка Вкладки Справка  
root@rm-02:~# asterisk -rvvv  
Privilege escalation protection disabled!  
See https://wiki.asterisk.org/wiki/x/1gKfAQ for more details.  
Asterisk 11.7.0-dfsg-lubuntu1, Copyright (C) 1999 - 2013 Digium, Inc. and others.  
Created by Mark Spencer <markster@digium.com>  
Asterisk comes with ABSOLUTELY NO WARRANTY; type 'core show warranty' for details.  
This is free software, with components licensed under the GNU General Public  
License version 2 and other licenses; you are welcome to redistribute it under  
certain conditions. Type 'core show license' for details.  
=====
```

```
Connected to Asterisk 11.7.0-dfsg-lubuntu1 currently running on rm-02 (pid = 8101)  
== Using SIP RTP CoS mark 5  
-- Executing [02@full:1] Dial("SIP/200000-00000000", "SIP/172.16.119.4/02") in new stack  
== Using SIP RTP CoS mark 5  
-- Called SIP/172.16.119.4/02  
-- SIP/172.16.119.4-00000001 answered SIP/200000-00000000  
-- Locally bridging SIP/200000-00000000 and SIP/172.16.119.4-00000001  
== Spawn extension (full, 02, 1) exited non-zero on 'SIP/200000-00000000'  
== Using SIP RTP CoS mark 5  
-- Executing [03@full:1] Dial("SIP/200000-00000002", "SIP/172.16.119.4/03") in new stack  
== Using SIP RTP CoS mark 5  
-- Called SIP/172.16.119.4/03  
-- SIP/172.16.119.4-00000003 answered SIP/200000-00000002  
-- Locally bridging SIP/200000-00000002 and SIP/172.16.119.4-00000003  
== Spawn extension (full, 03, 1) exited non-zero on 'SIP/200000-00000002'  
== Using SIP RTP CoS mark 5  
-- Executing [112@full:1] Dial("SIP/200000-00000004", "SIP/172.16.119.4/112") in new stack  
== Using SIP RTP CoS mark 5  
-- Called SIP/172.16.119.4/112  
-- SIP/172.16.119.4-00000005 answered SIP/200000-00000004  
-- Locally bridging SIP/200000-00000004 and SIP/172.16.119.4-00000005  
== Spawn extension (full, 112, 1) exited non-zero on 'SIP/200000-00000004'  
== Using SIP RTP CoS mark 5  
-- Executing [060@full:1] Dial("SIP/200000-00000006", "SIP/172.16.119.4/060") in new stack  
== Using SIP RTP CoS mark 5  
-- Called SIP/172.16.119.4/060  
-- SIP/172.16.119.4-00000007 answered SIP/200000-00000006  
-- Locally bridging SIP/200000-00000006 and SIP/172.16.119.4-00000007  
== Spawn extension (full, 060, 1) exited non-zero on 'SIP/200000-00000006'  
rm-02*CLI>
```

Рисунок 54 – Сообщения о ходе обработки вызовов, при обращении к узлу УСС

12. Выход из консоли управления Asterisk осуществляется командой *exit*.

Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и районированной ГТС без узлообразования с узлом УСС.

1.10 Лабораторная работа №9. «Построение сети связи. Организация сети при соединении двух АМТС, расположенных в разных городах».

В работе необходимо построить на полигоне СОТСБИ-NGN сеть связи в соответствии со схемой, заданной на (*Рисунок 55*). Схема включает в себя 2 районные автономные телефонные станции (РАТС), 2 узла спецслужб (УСС), учрежденческо-производственную АТС (УПАТС), 2 автоматических междугородных телефонных станций (АМТС), центральную станцию (ЦС) и 2 оконечные станции (ОС).

Каждое рабочее место представляет собой один из узлов на схеме и настраивает необходимые для корректной работы сети функции.

В работе участвует группа из десяти рабочих мест. Нумерация абонентов РАТС, ЦС и ОС шестизначная, УСС и УПАТС трехзначная, АМТС пятизначная и четырехзначная (таблица 8). Схема сети представлена на (*Рисунок 55*).

Для настройки соединения между РАТС, ОС, АМТС и УСС в качестве основы используйте файлы конфигурации из раздела «Настройка маршрутизации между двумя IP PBX Asterisk», для настройки работы УУС — раздел «Услуга “Точное время”», для маршрутизации между (РАТС №2 и УПАТС) — «Настройка маршрутизации между двумя IP PBX Asterisk (АТС и УПАТС)». Детализированный алгоритм организации сети при размещении двух АМТС, расположенных в разных городах в графическом виде представлен на (*Рисунок 56*).

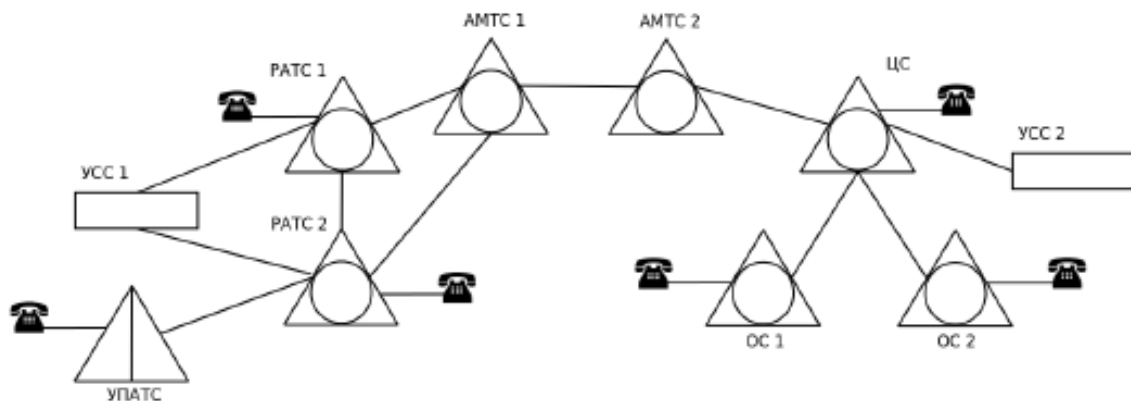


Рисунок 55 – Схема организации сети при размещении двух АМТС, расположенных в разных городах

Таблица 8. Нумерация на сети

№	Номер АТС	Нумерация (общая)	Нумерация	РМ, использующиеся в работе
1	ПАТС №1	1XXXXXX	100000	РМ №1
2	ПАТС №2	2XXXXXX	200000	РМ №2
3	УСС №1	0XX и 112	060, 02, 03 и 112	РМ №3
4	УПАТС	4XX	400, 401, 402	РМ №4
5	АМТС №1	XXXXX	1520	РМ №5
6	АМТС №2	XXXXXX	39100	РМ №6
7	ЦС	7XXXXXX	700000	РМ №7
8	ОС №1	8XXXXXX	800000	РМ №8
9	ОС №2	9XXXXXX	900000	РМ №9
10	УСС №2	0XX и 112	060, 02, 03 и 112	РМ №10

Для настройки УСС необходимо определить на нем функции служб, прописав адреса соответствующих звуковых файлов:

- 02 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_02
- 03 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_03
- 060 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja
- 112 —/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_112

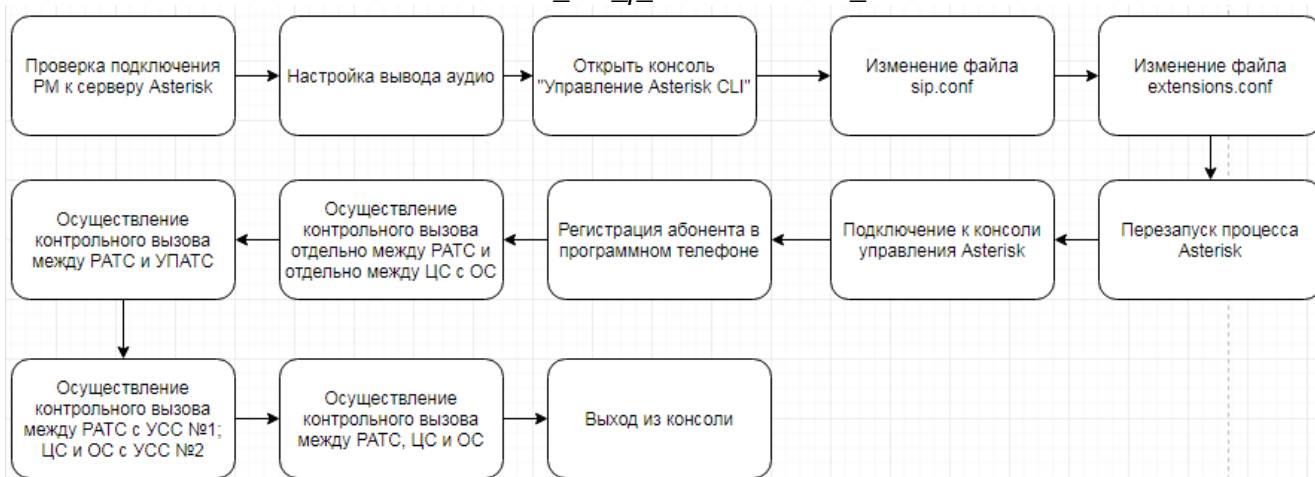


Рисунок 56 – Алгоритм организации сети при размещении двух АМТС, расположенных в разных городах

Алгоритм выполнения работы:

1. Перед выполнением работы необходимо удостовериться в том, что все РМ подключены к серверу Asterisk, для этого необходимо выполнить регистрацию двух пользователей на каждой РМ и выполнить контрольный межстанционный вызов в программных телефонах Twinkle и Linphone (приложение 4).

2. Перед выполнением работы необходимо удостовериться в том, что вывод аудио подключен и настроен (приложение 5).

3. Для построения сети связи необходимо изменить настройки, хранящиеся в файлах /etc/asterisk/sip.conf и /etc/asterisk/extensions.conf. Для этого необходимо зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

4. В файл /etc/asterisk/sip.conf добавить 10 абонентов с номерами, соответствующими таблице 8. Пример содержимого файлов:

PATC №1-2, ЦС, ОС №1,2:

sip.conf (шаблон)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

[172.16.119.X](!)

```
type=friend
host=dynamic
context=full
disallow=all
allow=alaw
```

```
[Y00000](172.16.119.X)
[Y00001](172.16.119.X)
```

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

```
[Y00000](172.16.119.X)
[Y00001](172.16.119.X)
```

[172.16.119.X]

sip.conf (PATC №1)

```
[general]
allowguest=no
udpbindaddr=172.16.119.151
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

[172.16.119.1](!)

```
type=friend
host=dynamic
context=full
disallow=all
allow=alaw
```

```
[100000](172.16.119.1)
[100001](172.16.119.1)
```

```
[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw
```

```
[200000](172.16.119.2)
[200001](172.16.119.2)
```

[172.16.119.3]

type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

type=friend
host=172.16.119.153
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[172.16.119.5]
type=friend
host=172.16.119.155
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

Для ЦС добавляется характеристика для ОС №2, которая заполняется также как и в ПАТС:

sip.conf (шаблон)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[Y00000](172.16.119.X)
[Y00001](172.16.119.X)

sip.conf (ЦС)

[172.16.119.9]
type=friend
host=172.16.119.159
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[900000](172.16.119.9)
[900001](172.16.119.9)

Для ПАТС №2, которая связана с УПАТС добавляются следующие строки:

sip.conf (шаблон)

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[Y00](172.16.119.X)
[Y01](172.16.119.X)
[Y02](172.16.119.X)

sip.conf (ПАТС №2)

[172.16.119.4]
type=friend
host=172.16.119.154
port=5060
canreinvite=no
context=full
disallow=all
allow=alaw

[400](172.16.119.4)
[401](172.16.119.4)
[402](172.16.119.4)

В ОС прописывается характеристика самой ОС так же, как и для РАТС и характеристика для ЦС.

УСС:

sip.conf (шаблон) УСС

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw
```

```
[Y00000](172.16.119.X)
[Y00001](172.16.119.X)
```

```
[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw
```

```
[Y00000](172.16.119.X)
[Y00001](172.16.119.X)
```

sip.conf (РМ №3) УСС

```
[general]
allowguest=no
udpbindaddr=172.16.119.153
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru
```

```
[172.16.119.1]
type=friend
host=172.16.119.151
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw
```

```
[100000](172.16.119.1)
[100001](172.16.119.1)
```

```
[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=internal
disallow=all
allow=alaw
```

```
[200000](172.16.119.2)
[200001](172.16.119.1)
```

Для РМ10 прописывается характеристика только для одной РМ №7, а не для двух.

УПАТС:

sip.conf (шаблон) УПАТС

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
```

sip.conf (РМ9) УПАТС

```
[general]
allowguest=no
udpbindaddr=172.16.119.154
transport=udp
srvlookup=yes
disallow=all
```

*allow=alaw
allow=ulaw
language=ru*

*[172.16.119.X](!)
type=friend
host=dynamic
context=pbx
disallow=all
allow=alaw*

*[400](172.16.119.X)
[401](172.16.119.X)
[402](172.16.119.X)
[403](172.16.119.X)*

*[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context=voice_menu
disallow=all
allow=alaw*

*[Y00000](172.16.119.X)
[Y00001](172.16.119.X)*

*allow=alaw
allow=ulaw
language=ru*

*[172.16.119.4](!)
type=friend
host=dynamic
context=pbx
disallow=all
allow=alaw*

*[400](172.16.119.4)
[401](172.16.119.4)
[402](172.16.119.4)
[403](172.16.119.4)*

*[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=voice_menu
disallow=all
allow=alaw*

*[200000](172.16.119.2)
[200001](172.16.119.2)*

AMTC №1-2:

sip.conf (шаблон)

*[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru*

*[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context= external*

sip.conf (AMTC1)

*[general]
allowguest=no
udpbindaddr=172.16.119.155
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
language=ru*

*[172.16.119.1]
type=friend
host=172.16.119.151
port=5060
canreinvite=no
context=external*

disallow=all
allow=alaw

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context= external
disallow=all
allow=alaw

[172.16.119.X]
type=friend
host=172.16.119.Z
port=5060
canreinvite=no
context= external
disallow=all
allow=alaw

disallow=all
allow=alaw

[172.16.119.2]
type=friend
host=172.16.119.152
port=5060
canreinvite=no
context=external
disallow=all
allow=alaw

[172.16.119.6]
type=friend
host=172.16.119.156
port=5060
canreinvite=no
context=external
disallow=all
allow=alaw

Для АМТС 2 прописывается характеристика для ЦС вместо РАТС №1-2.

В шаблоне файла *sip.conf* вместо символов *X* прописывается последнее число IP-адреса РМ, *Y* - первая цифра из нумерации РМ в сети (таблица 8), *Z* – последнее число адреса РМ на сервере Asterisk. В файле *sip.conf* для УПАТС прописаны дополнительные номера 902 и 903, но в работе не используются.

5. В файлы */etc/asterisk/extensions.conf* добавить правила обработки вызовов:
extensions.conf (шаблон) РАТС №1-2:

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no

[internal]
exten => X00000,1,Dial(SIP/${EXTEN})
exten => X00000,n,Hangup()

[external]
exten => X00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => X00000,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 02,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 03,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 060,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 112,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
```

```

exten => 8DY00000,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
exten => 8DY00000,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
exten => 8DY00000,n,Hangup()
exten => 599900,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 599900,n,Hangup()
[full]
include => internal
include => external

```

В файле *extensions.conf* (ПАТС1) не прописываются следующие строки:

```

exten => 599900,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 599900,n,Hangup()

```

extensions.conf (ПАТС №2):

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 200000,1,Dial(SIP/${EXTEN})
exten => 200000,n,Hangup()
[external]
exten => 100000,1,Dial(SIP/172.16.119.151/${EXTEN})
exten => 100000,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.153/${EXTEN})
exten => 112,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119.153/${EXTEN})
exten => 060,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.153/${EXTEN})
exten => 03,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.153/${EXTEN})
exten => 02,n,Hangup()
exten => 839100700000,1,Dial(SIP/172.16.119.155/${EXTEN:1})
exten => 839100700000,n,Hangup()
exten => 839100800000,1,Dial(SIP/172.16.119.155/${EXTEN:1})
exten => 839100800000,n,Hangup()
exten => 839100900000,1,Dial(SIP/172.16.119.155/${EXTEN:1})
exten => 839100900000,n,Hangup()
exten => 599900,1,Dial(SIP/172.16.119.154/${EXTEN})
exten => 599900,n,Hangup()
[full]
include => internal
include => external

```

extensions.conf (YCC №1,2):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 060,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/vremja)
exten => 060,n,SayUnixTime(,HM)
exten => 060,n,Hangup()
exten => 02,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_02)
exten => 02,n,Hangup()
exten => 03,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_03)
exten => 03,n,Hangup()
exten => 112,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ssn_112)
exten => 112,n,Hangup()
```

extensions.conf (шаблон)УПАТС:

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[voice_menu]
exten => 599900,1,Answer()
exten => 599900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/thank-you-for-calling)
exten => 599900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/to-contact-sales)
exten => 599900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/najmite-1)
exten => 599900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/to-contact-tech-support)
exten => 599900,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/najmite-2)
exten => 599900,n,WaitExten(5)
exten => 1,1,Dial(SIP/401,10)
exten => 1,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ne-otvechaet)
exten => 1,n,Hangup()
exten => 2,1,Dial(SIP/402,10)
exten => 2,n,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/ne-otvechaet)
exten => 2,n,Hangup()
exten => i,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/nevernyj-vybor)
exten => i,n,Goto(voice_menu,399900,1)
exten => t,1,Playback(/usr/share/asterisk/sounds/ru_RU_f_IvrvoiceRU/do-svidanija)
exten => t,n,Hangup()

[internal]
exten => Y00,1,Dial(SIP/${EXTEN})
exten => Y00,n,Hangup()
[external]
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
```

```

exten => Y00000,n,Hangup()
[pbx]
include => internal
include => external

```

В работе в файле *extensions.conf* для УПАТС на РМ9 были изменены значения шаблона в областях *[internal]* и *[external]*:

```

[internal]
exten => 900,1,Dial(SIP/${EXTEN})
exten => 900,n,Hangup()
[external]
exten => 200000,1,Dial(SIP/172.16.119.2/${EXTEN:1})
exten => 200000,n,Hangup()

```

extensions.conf (шаблон) **АМТС**:

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[external]
exten => DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:4})
exten => DY00000,n,Hangup()
exten => DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:4})
exten => DY00000,n,Hangup()
exten => DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => DY00000,n,Hangup()
exten => DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => DY00000,n,Hangup()
exten => DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => DY00000,n,Hangup()

```

extensions.conf АМТС №1:

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no

[external]
exten => 1520100000,1,Dial(SIP/172.16.119.151/${EXTEN:4})
exten => 1520100000,n,Hangup()
exten => 1520200000,1,Dial(SIP/172.16.119.152/${EXTEN:4})
exten => 1520200000,n,Hangup()
exten => 39100700000,1,Dial(SIP/172.16.119.156/${EXTEN})
exten => 39100700000,n,Hangup()
exten => 39100800000,1,Dial(SIP/172.16.119.156/${EXTEN})
exten => 39100800000,n,Hangup()

```

```
exten => 39100900000,1,Dial(SIP/172.16.119.156/${EXTEN})
exten => 39100900000,n,Hangup()
```

extensions.conf **AMTC №2:**

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[external]
exten => 1520100000,1,Dial(SIP/172.16.119.155/${EXTEN})
exten => 1520100000,n,Hangup()
exten => 1520200000,1,Dial(SIP/172.16.119.155/${EXTEN})
exten => 1520200000,n,Hangup()
exten => 39100700000,1,Dial(SIP/172.16.119.157/${EXTEN:5})
exten => 39100700000,n,Hangup()
exten => 39100800000,1,Dial(SIP/172.16.119.157/${EXTEN:5})
exten => 39100800000,n,Hangup()
exten => 39100800000,1,Dial(SIP/172.16.119.157/${EXTEN:5})
exten => 39100800000,n,Hangup()
```

extensions.conf (шаблон) **ЦС:**

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => X00000,1,Dial(SIP/${EXTEN})
exten => X00000,n,Hangup()
[external]
exten => X00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => X00000,n,Hangup()
exten => X00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => X00000,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 02,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 03,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 060,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 112,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
exten => 8DY00000,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN:1})
exten => 8DY00000,n,Hangup()
```

```
[full]
include => internal
include => external
```

extensions.conf **UC:**

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 700000,1,Dial(SIP/${EXTEN})
exten => 700000,n,Hangup()
[external]
exten => 800000,1,Dial(SIP/172.16.119.158/${EXTEN})
exten => 800000,n,Hangup()
exten => 900000,1,Dial(SIP/172.16.119.159/${EXTEN})
exten => 900000,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.160/${EXTEN})
exten => 112,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119.160/${EXTEN})
exten => 060,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.160/${EXTEN})
exten => 03,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.160/${EXTEN})
exten => 02,n,Hangup()
exten => 81520100000,1,Dial(SIP/172.16.119.156/${EXTEN:1})
exten => 81520100000,n,Hangup()
exten => 81520200000,1,Dial(SIP/172.16.119.156/${EXTEN:1})
exten => 81520200000,n,Hangup()
[full]
include => internal
include => external
```

extensions.conf (шаблон) **OC:**

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => Y00000,1,Dial(SIP/${EXTEN})
exten => Y00000,n,Hangup()
[external]
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => Y00000,n,Hangup()
exten => Y00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
```

```

exten => Y00000,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 02,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 03,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 060,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 112,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 8DY00000,n,Hangup()
exten => 8DY00000,1,Dial(SIP/172.16.119.Z/${EXTEN})
exten => 8DY00000,n,Hangup()
[full]
include => internal
include => external

```

В файле *extensions.conf* (OC) вместо Z прописывается последнее число адреса РМ на сервере Asterisk для ЦС.

extensions.conf **OC 1:**

```

[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 800000,1,Dial(SIP/${EXTEN})
exten => 800000,n,Hangup()
[external]
exten => 700000,1,Dial(SIP/172.16.119.157/${EXTEN})
exten => 700000,n,Hangup()
exten => 900000,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 900000,n,Hangup()
exten => 112,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 112,n,Hangup()
exten => 060,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 060,n,Hangup()
exten => 03,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 03,n,Hangup()
exten => 02,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 02,n,Hangup()
exten => 81520100000,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 81520100000,n,Hangup()
exten => 81520200000,1,Dial(SIP/172.16.119. 157/${EXTEN})
exten => 81520200000,n,Hangup()
[full]
include => internal

```

include => external

В шаблоне файла *extensions.conf* вместо символов *Y* прописывается первая цифра из нумерации РМ в сети (таблица 8), *Z* – последнее число адреса РМ на сервере Asterisk, *D* – полный номер АМТС.

Содержание файлов конфигурации подробно описано в приложении 6.

6. Перезапустить процесс *asterisk* командой */etc/init.d/asterisk restart* (Рисунок 25).

7. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (Рисунок 25).

8. На РМ №1-2,4,7-9 запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» установить порт *UDP 5062*, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером РМ в соответствии с таблицей 8 (приложение 2). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента.

9. Выполнить контрольный межстанционный вызов между РАТС №1-2 и отдельно между ЦС и ОС №1-2. В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова. В качестве адресов использовать нумерацию в сети из таблицы 8.

10. Выполнить контрольный межстанционный вызов между РАТС №2 и УПАТС. Для этого использовать в качестве адреса «399900». При вызове прослушать информацию о сотрудниках и после её окончания нажать 1 или 2 для соединения с оператором. Для ввода цифр во время звонка нажать «Вывод клавиатуры» в меню «Опции». В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (Рисунок 57).

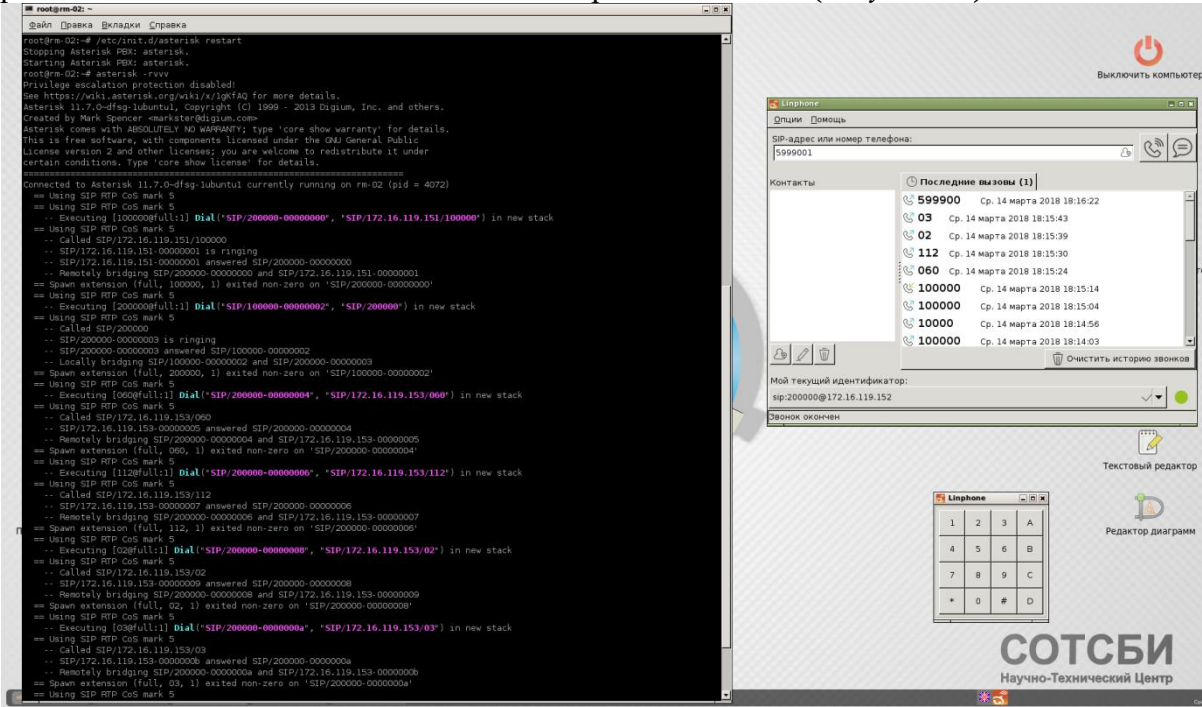


Рисунок 57 – Сообщения о ходе обработки вызовов, при обращении к узлу УПАТС и РАТС №2

11. Выполнить контрольный межстанционный вызов между РАТС №1-2 и УСС №1 и, отдельно, ЦС, ОС №1-2 и УСС №2. Для этого использовать в качестве адреса нумерацию подключенных служб (таблица 8). При вызове данных служб будет слышен:

«060» - говорится, женским голосом, точное время, установленное в системе;

«02» - фраза «полиция», сказанная мужским голосом;

«03» - фраза «скорая медицинская помощь», сказанная женским голосом;

«112» - фраза «экстренные оперативные службы», сказанная мужским голосом.

В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки вызова (Рисунок 58)

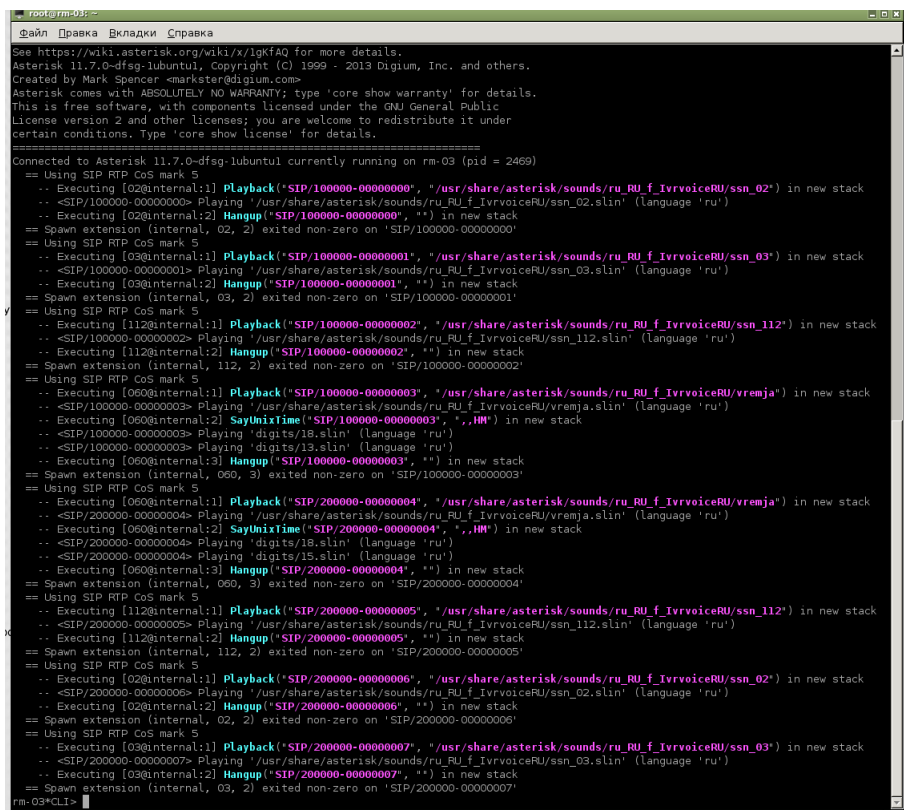


Рисунок 58 – Сообщения о ходе обработки вызовов, при обращении к узлу УСС

12. Выполнить контрольный межстанционный вызов между РАТС №1-2 и ЦС, ОС №1-2. Для этого на РАТС №1-2 набрать номер 8DY00000, где *D* – это номер АМТС в другой зоне, в данном случае АМТС 6 с номером 39100, а *Y* – это первая цифра номера РМ на которую поступит вызов (например: 700000). Пример номера на РАТС №1-2: 839100700000. Аналогично для ЦС и ОС №1-2, но с номером АМТС №1 (номер АМТС №1: 1520). Пример номера на ЦС и ОС №1-2: 815202000000 (Рисунок 59) ().

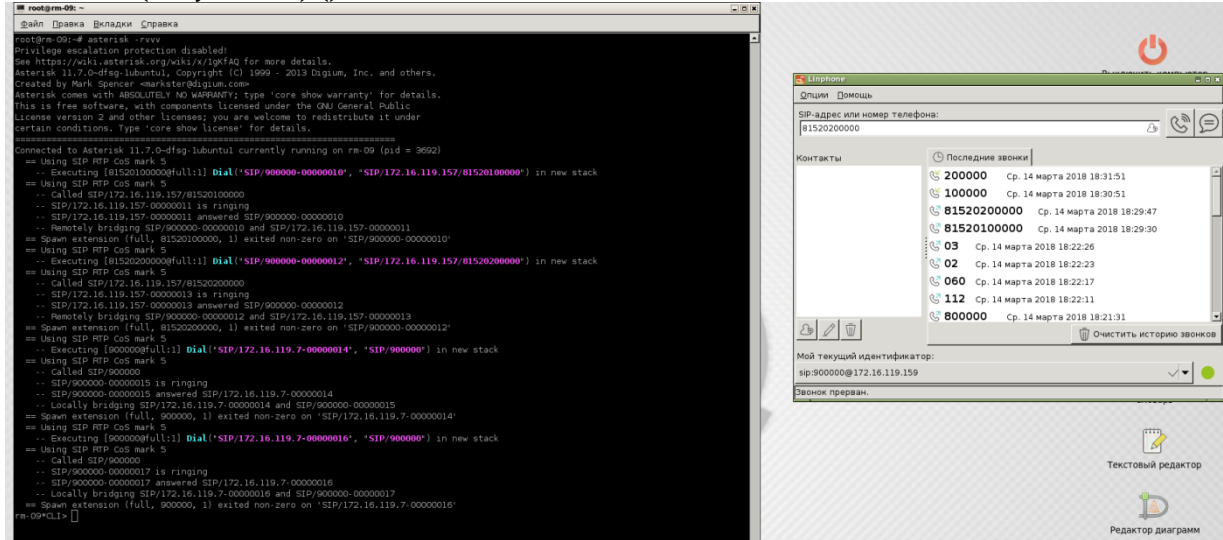


Рисунок 59 – Сообщения о ходе обработки вызовов, при вызове РАТС через АМТС с ОС №2

13. Выход из консоли управления Asterisk осуществляется командой *exit*. Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и сети при размещении двух АМТС, расположенных в разных городах.

Часть 2. «Сети NGN. Оборудование IMS»

Лабораторная работа №1 «Процедура регистрации»

Регистрация является основной процедурой любой сети IMS. Если пользователи не зарегистрированы, тогда они не смогут получить доступ к любым сервисам сети. Для успешной регистрации пользователь должен обладать определенными регистрационными данными, а сеть, в которой производится процесс регистрации, должна быть доступна для приема этих регистрационных данных. Данная лабораторная работа состоит из нескольких заданий, главная цель которой — проанализировать процедуру регистрации в сети IMS, определить основные элементы сети IMS, участвующие в процедуре регистрации, и протоколы взаимодействия.

Создание пользователя

Прежде чем зарегистрировать пользователя в сети IMS, необходимо создать информацию об этом пользователе в базе данных пользователей HSS. Создание пользователей, редактирование и управление конфигурационными данными пользователей в HSS осуществляется с помощью web-интерфейса HSS.

1. Запустить web-интерфейс HSS. Для авторизации ввести логин *hssAdmin* и пароль *hss* (Рисунок 60).

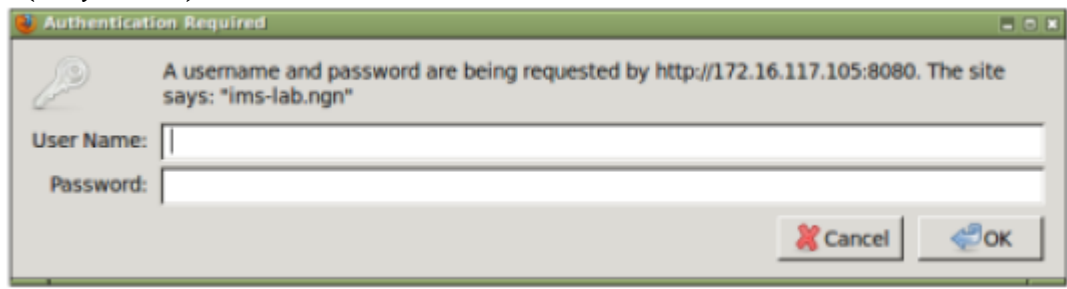


Рисунок 60 – Авторизация в HSS

2. Создать пользователя с именем *User1* и таким же паролем.
2.1. Для создания информации о пользователе в базе данных пользователей HSS необходимо выбрать пункт меню «Пользователи IMS». Затем выбрать подпункт меню «Пользователи IMS» —Создание (Рисунок 61).

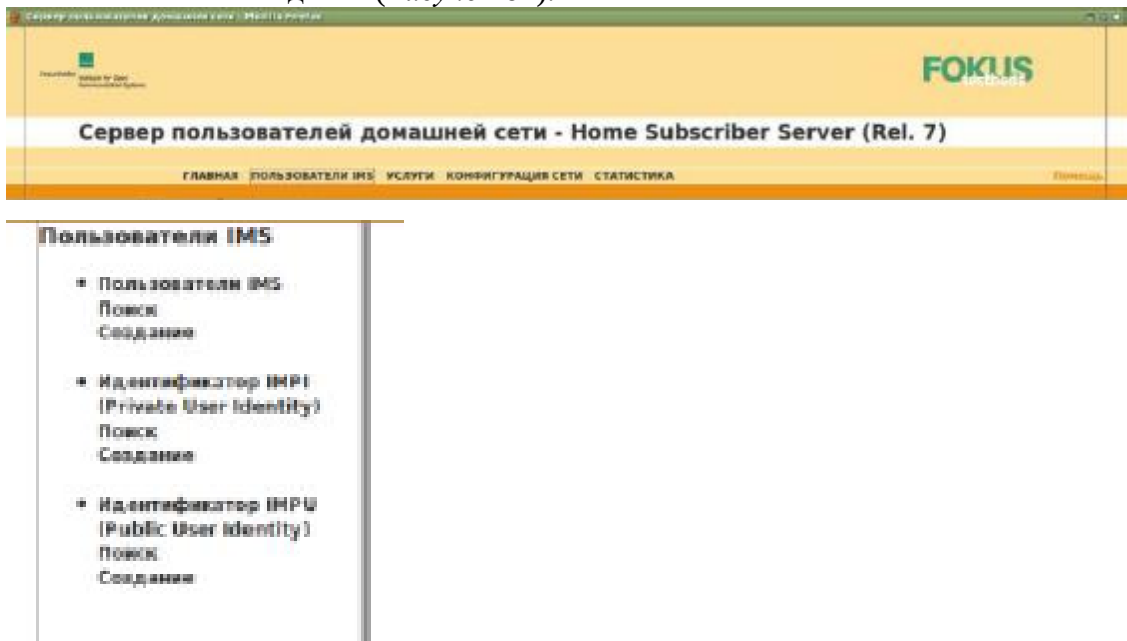


Рисунок 61 – Web-интерфейс HSS

- 2.2. В появившемся окне отображается таблица, поля которой необходимо заполнить. В поле «Имя пользователя» необходимо ввести имя пользователя *User1* английскими

строчными буквами. В поле «Набор идентификаторов сервисов» необходимо выбрать значение cap_set1, а в поле «Предпочтительный S-CSCF» — значение scscf1 и нажать кнопку «Сохранить» (Рисунок 62).

Создание пользователя IMS -IMSU-

ID	1
Имя пользователя *	
Набор идентификаторов сервисов	cap_set1
Предпочтительный S-CSCF	scscf1
Доменное имя S-CSCF	
Diameter Name	

Обязательное поле *

Сохранить Обновить Очистить

Рисунок 62 – Создание пользователя IMS

2.3. Далее необходимо прописать идентификатор Private User Identity для создаваемого пользователя. Для этого необходимо нажать значок «+», расположенный справа от пункта «Создание и присвоение нового идентификатора IMPI» (Рисунок 63).

Создание пользователя IMS -IMSU-

ID	23
Имя пользователя *	user333
Набор идентификаторов сервисов	cap_set1
Предпочтительный S-CSCF	scscf1
Доменное имя S-CSCF	
Diameter Name	

Обязательное поле *

Создание и присвоение нового идентификатора IMPI +

Присвоение IMPI

Идентификатор IMPI		Добавить
--------------------	--	----------

Список присвоенных идентификаторов IMPI

ID	Идентификатор IMPI	Удалить
----	--------------------	---------

Сохранить Обновить Удалить

Рисунок 63 – Присвоение идентификатора

В появившемся окне в поле «Идентификатор IMPI» необходимо ввести идентификатор *Private User Identity* вида **user1@ngn.lab**. В поле «Секретный ключ» —пароль пользователя *user1* для доступа создаваемого пользователя в сеть. Затем выбрать все алгоритмы аутентификации, отметив соответствующее поле, а из выпадающего списка «По умолчанию» —значение *Digest-AKAv1-MD5* и нажать кнопку «Сохранить» (Рисунок 64).

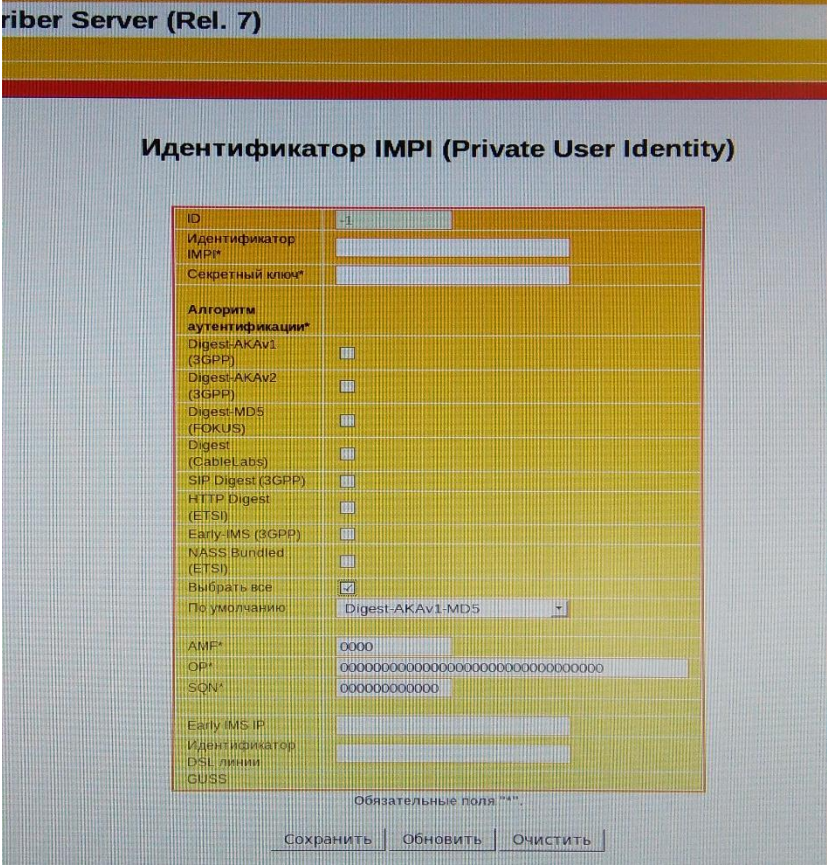


Рисунок 64 – Заполнение полей идентификатора

2.4.Затем необходимо прописать идентификатор *Public User Identity* для создаваемого пользователя. Для этого необходимо нажать значок «+», расположенный справа от пункта «Создание и присвоение нового идентификатора *IMPU*».

В появившемся окне в поле Идентификатор *IMPU* необходимо ввести идентификатор *Public User Identity* вида *sip:user1@ims-lab.ngn*. Из выпадающего списка поля «Профиль обслуживания» выбрать значение *default_sp*. Для поддержки возможности регистрации установить флажок в поле «Разрешить регистрацию». В поле тип *IMPU* выбрать значение *Public_User_Identity*, а в поле «Отображаемое имя пользователя» ввести отображаемое имя создаваемого пользователя *user1* и нажать кнопку «Сохранить» (Рисунок 65).

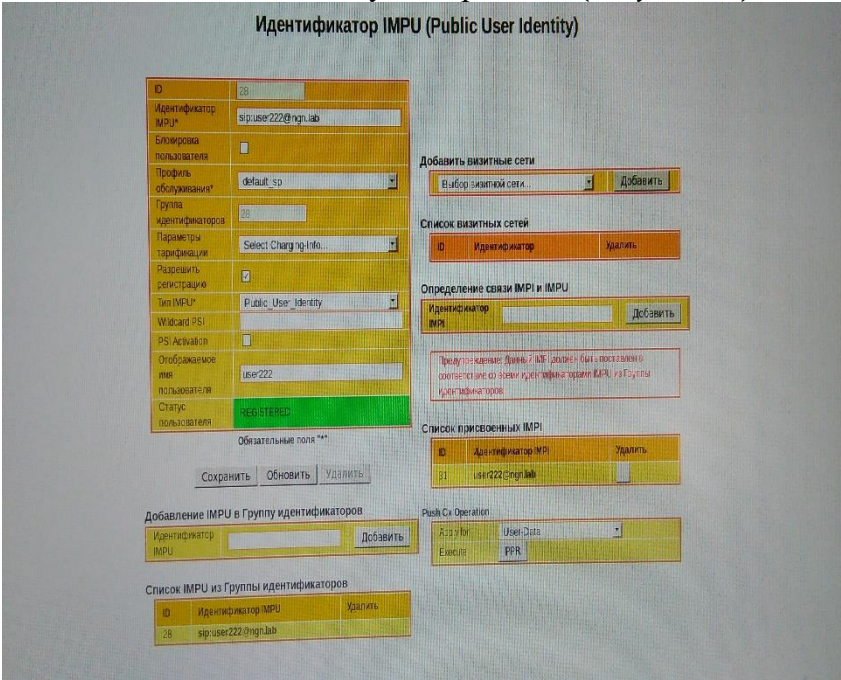


Рисунок 65 – Назначение идентификатора *Public User Identity* для создаваемого пользователя.

2.5. В поле «Добавить визитные сети» необходимо выбрать значение *ngn.lab*, нажать кнопку «Добавить» и далее кнопку «Сохранить» (Рисунок 66).

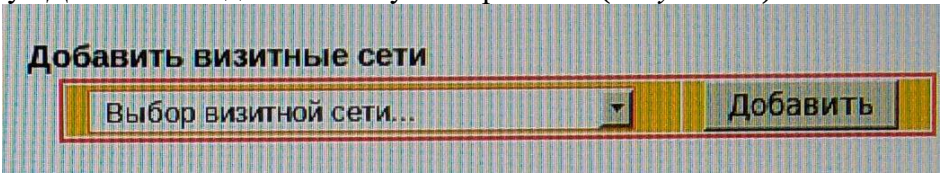


Рисунок 66 – Добавление визитной сети

Регистрация

Определение местоположения пользователя сети IMS в текущий момент осуществляется с помощью процедуры регистрации. Так как пользователь регистрируется в сети IMS впервые, то ему необходимо пройти процедуру аутентификации.

- 1. Запустить *Wireshark* (Рисунок 67).

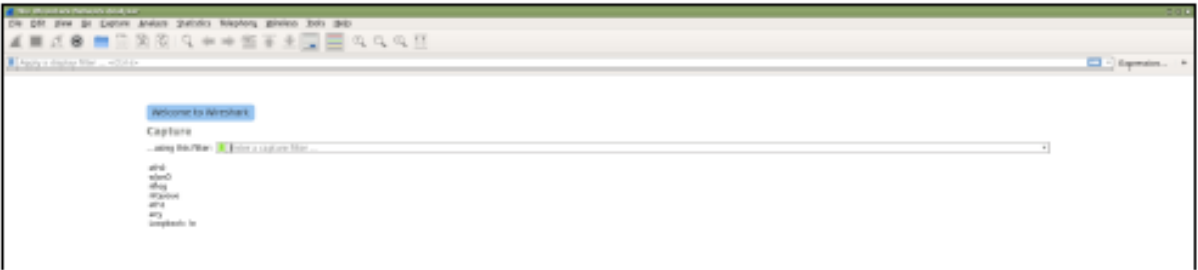


Рисунок 67 – Запуск Wireshark

- 2. Настроить терминал IMS Monster. Открываем терминал IMS-клиент Monster (Рисунок 68).

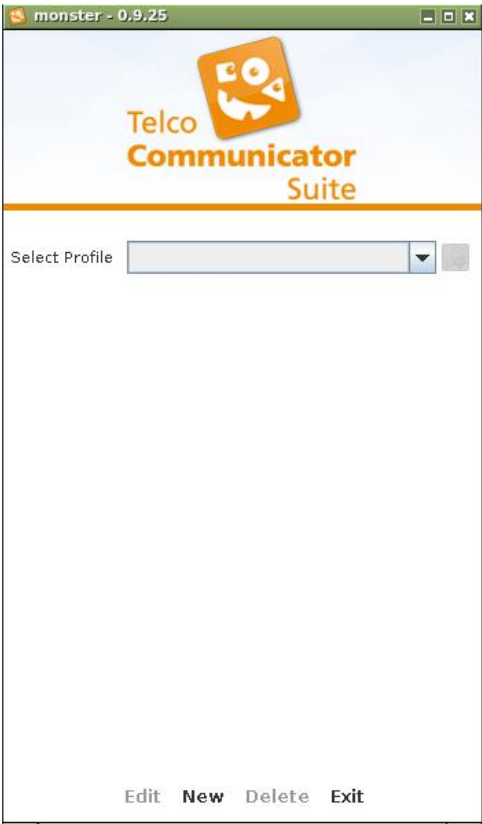


Рисунок 68 – Открытие терминала IMS-клиент Monster

3. Для создания нового профиля нужно нажать на кнопку *New*, расположенную в нижней части окна. Появляется новое окно (Рисунок 69):

Preference Settings

IMS Network

Configuration parameters for the IMS network and discovery.
NOTE: Changes made here while you are registered, will only take effect, the next time you sign in again.

Connection settings

The domain of your IMS network
ngn.lab

Display name
Alice

Public Identity
sip:sp91_3791@ngn.lab

Private Identity
sp91_3791@ngn.lab

Secret key

PCSCF
pcscf.ngn.lab

PCSCF Port
4060

Discovery settings

PCSCF Discovery
DNS

Local settings (optional)

Local IP address
[empty field]

Local port
5060

Profile name: dummyFileName **save**

Рисунок 69 – Создание нового профиля

В этом окне указываем следующие значения:

Domain: *ngn.lab*

Display name: *ваше имя*

Public Identity: *sip:ваше_имя@ngn.lab*

Private Identity: *ваше_имя@ngn.lab*

Secret key: *ваш пароль*

PCSCF: *pcscf.ngn.lab*

PCSCF Port: *4060*

PCSCF Discovery: *DNS*

Local port: *5060*

Profile name: *отображаемое имя*

4. Далее нажимаем *save*.

5. Чтобы войти в программу в поле *Select Profile* выбираем ваш профиль и нажимаем войти (кнопка справа от поля с именем) (Рисунок 70).

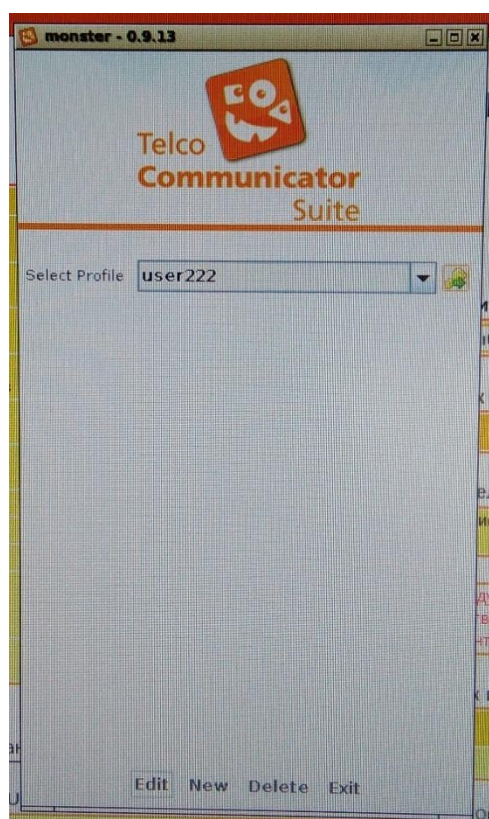


Рисунок 70 – Вход в программу Monster

6. Если все действие выполнены верно, то в результате получается следующее окно (Рисунок 71).

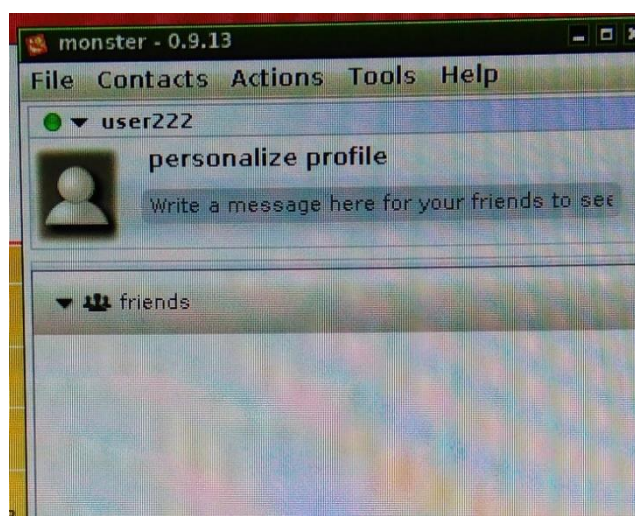


Рисунок 71 – Окно профиля User222

А также в web-интерфейсе HSS информация о пользователе будет отображаться с надписью **REGISTERED** (Рисунок 72).

Сервер пользователей домашней сети - Home Subscriber Server (Rel. 7)

ГЛАВНАЯ

ПОЛЬЗОВАТЕЛИ IMS

УСЛУГИ

КОНФИГУРАЦИЯ СЕТИ

СТАТИСТИКА

Пользователи IMS

Пользователи IMS

Поиск

Создание

Идентификатор IMPU (Private User Identity)

Поиск

Создание

Идентификатор IMPU (Public User Identity)

Поиск

Создание

Идентификатор IMPU (Public User Identity)

ID

20

Идентификатор IMPU*

sip:rostov.m@ims-lab.ngn

Блокировка пользователя

☐

Профиль обслуживания*

default_sp

Группа

20

Параметры тарификации

Select Charging-Info...

Разрешить регистрацию

☒

Тип IMPU*

Public_User_Identity

Wildcard PSI

PSI Activation

☐

Отображаемое имя пользователя

rostov m

Статус пользователя

NOT-REGISTERED

Обязательные поля **

Сохранить

Обновить

Удалить

Добавление IMPU в Группу идентификаторов

Идентификатор IMPU

Добавить

Список IMPU из Группы идентификаторов

ID	Идентификатор IMPU	Удалить
20	sip:rostov.m@ims-lab.ngn	

Добавить визитные сети

Выбор визитной сети...

Добавить

Список визитных сетей

ID	Идентификатор	Удалить
----	---------------	---------

Определение связи IMPU и IMPU

Идентификатор IMPU

Добавить

Предупреждение: Данный IMPU должен быть поставлен в соответствие со всеми идентификаторами IMPU из Группы идентификаторов!

Список присвоенных IMPU

ID	Идентификатор IMPU	Удалить
23	rostov.m@ims-lab.ngn	

Push Cx Operation

Apply for

User-Data

Execute

PPR

Рисунок 74 – Процедура регистрации пользователя в сети IMS

В окне настройки профиля пользователя (Рисунок 75) в левой части отображены разделы меню, а в правой содержимое выбранного раздела. Для настроек параметров подключения необходимо выбрать раздел меню *IMS Network*, в котором заполняются следующие поля:

- в поле *The domain of your IMS network* необходимо ввести имя домена сети *IMS – ngn.lab*;
- в поле *Display name* вводится имя вызывающего пользователя, которое будет отображаться на дисплее терминала вызываемого абонента;
- в поле *Public Identity* вводится идентификатор *Public Identity* пользователя;
- в поле *Private Identity* вводится идентификатор *Private Identity* пользователя;
- в поле *Secret Key* вводится пароль для аутентификации пользователя в сети;
- в поле *PCSCF* вводится адрес SIP-сервера – *pcscf.ngn.lab*;
- в поле *PCSCF Port* вводится номер порта SIP-сервера - 5060;
- в подразделе *Discovery setting* задаются настройки обнаружения входной точки в сеть IMS (обнаружение функции *pcscf* ядра сети). Для этого необходимо в поле *PCSCF Discovery* выбрать значение *DNS*;
- в подразделе *Local settings* в поле *Local port* необходимо ввести номер локального порта пользователя - 5060;
- в подразделе *SIP signaling options* задаются настройки сигнализации. Для возможности регистрации пользователя в сети необходимо рядом с полем *Send registration* поставить «галочку» и поле *Registration Time* ввести время регистрации.

После настройки всех параметров необходимо в поле *Profile name* ввести название профиля и нажать кнопку *Save*.

74

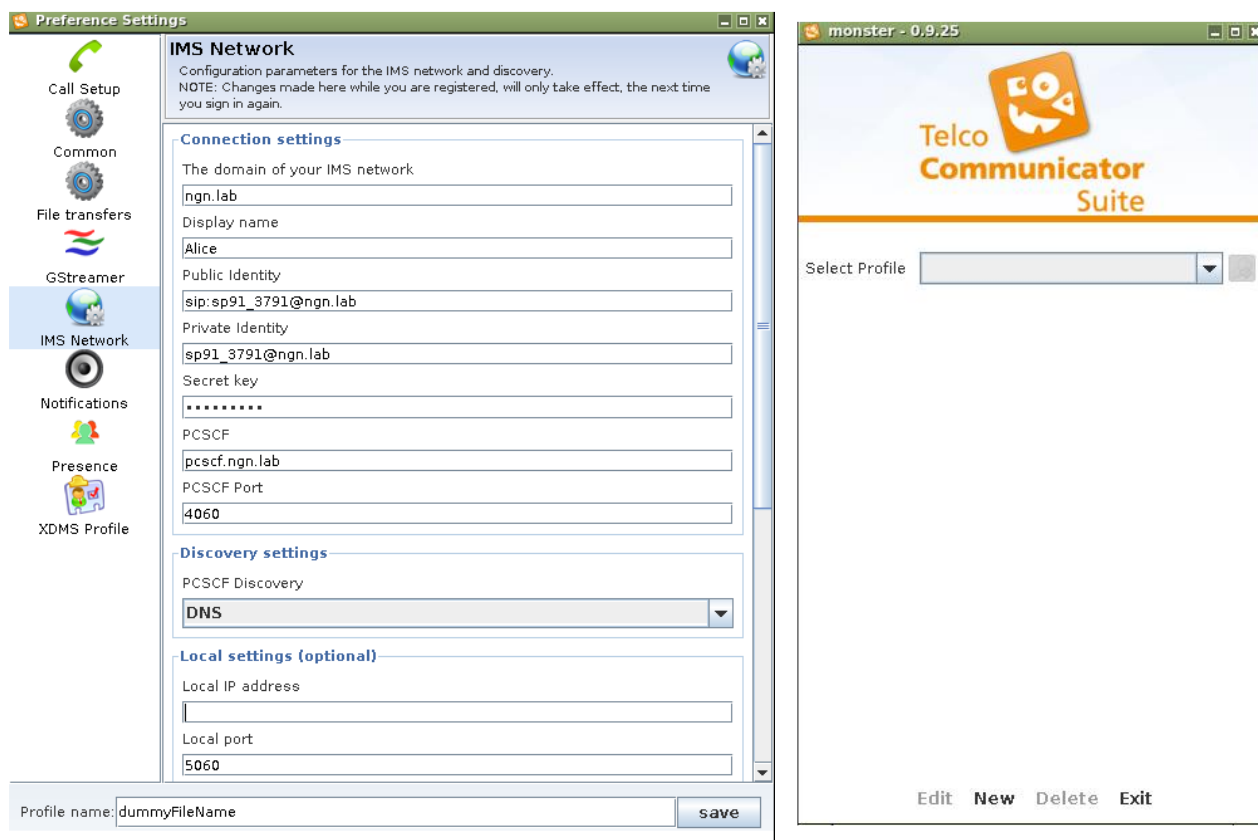


Рисунок 75 – Окно настройки профиля пользователя в Monster IMS

Далее требуется установить мультимедийную сессию между зарегистрированными пользователями IMS, находящимися в домашних сетях. IP-адрес рабочего места А будет 172.16.119.3 IP-адрес рабочего места В будет 172.16.119.4. Необходимо пройти регистрацию в программе Monster IMS, заполняя данные в каждом из полей, в соответствии с указанными там данными и IP адресом рабочего места.

Далее запускаем Wireshark (Рисунок 76).

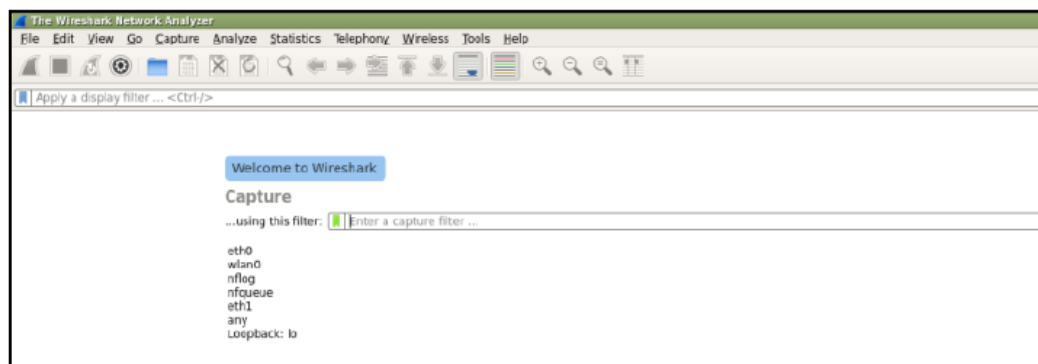


Рисунок 76 – Стартовое окно программы Wireshark

Совершаем звонок в программе Monster IMS.

Установление аудио/видео сессии можно осуществить двумя способами:

1. С помощью вкладки *Call* Главного окна (*Рисунок 77*)

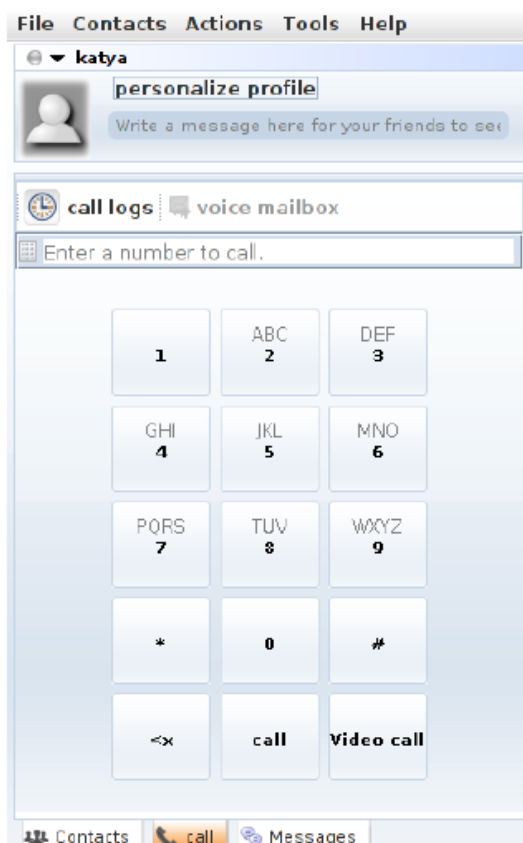


Рисунок 77 – Вкладка *Call* Главного окна

Для осуществления исходящей сессии необходимо ввести данные вызываемого пользователя в формате *sip:UserName@ngn.lab11* в поле для ввода номера и нажать кнопку *Call* для установления аудиосессии или *Video Call* для видеосессии.

2. С помощью вкладки *Contacts* главного окна (*Рисунок 78*).

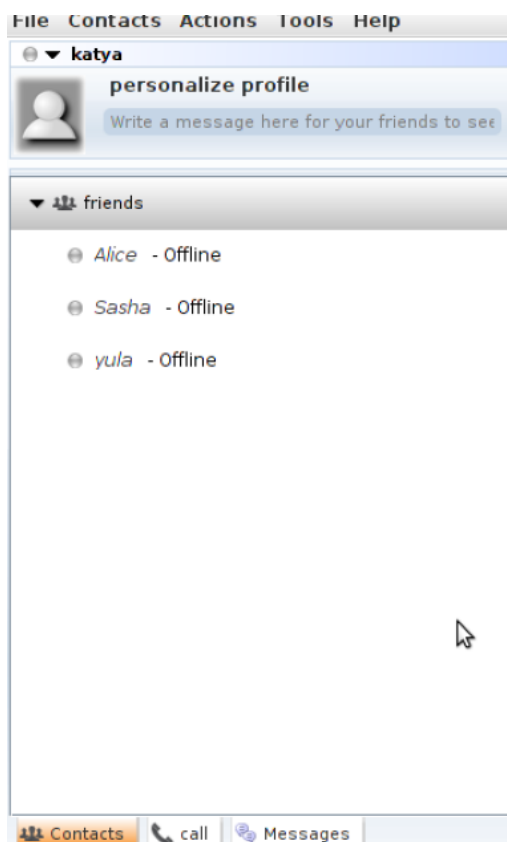


Рисунок 78 – Главное окно Monster

Для осуществления исходящей сессии необходимо выбрать абонента (предварительно добавленного в список контактов). В меню *Actions* выбрать *Place audio call* для установления аудиосессии или *Place video call* для видеосессии.

После ответа вызываемого абонента, панель состояния пользователя отображает имя вызываемого пользователя, а в случае видеовызова изображение пользователя появляется в окне Video (в случае если у вызываемого абонента установлена видеокамера) (Рисунок 79).

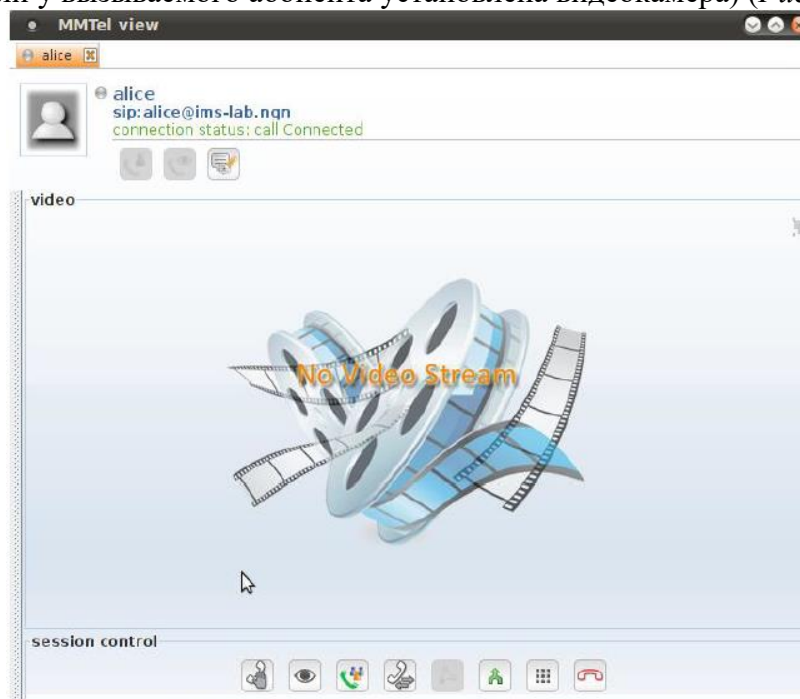


Рисунок 79 – Окно при установленной аудиосессии

Для разрушения сессии на любом этапе (отбой вызывающего пользователя) необходимо нажать кнопку *Hung up* (Разъединение) (кнопка с изображением красной телефонной трубки),

расположенную на панели *Session control*.

При поступлении входящего вызова появляется всплывающее окно *Incoming call*, содержащее кнопки *Accept* (Принять вызов), *Reject* (Отбой) (Рисунок 80).

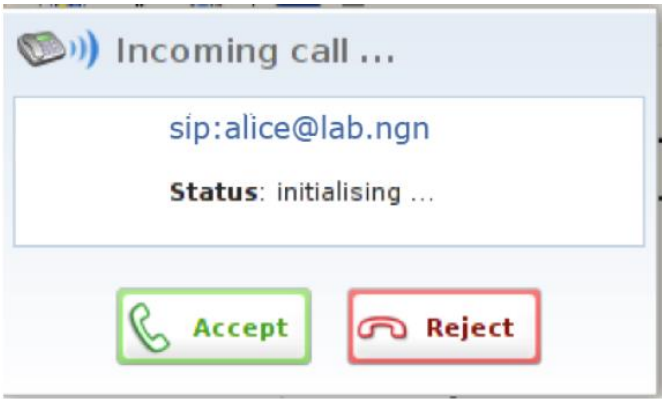


Рисунок 80 – Всплывающее окно при поступлении входящего сессии

Осуществляем фильтрацию по проколу SIP в Wireshark (Рисунок 81).

2187	49.404434830	172.16.119.4	172.16.119.3	SIP/SDP	842	Request: INVITE sip:172.16.119.3
2189	49.526995695	172.16.119.3	172.16.119.4	SIP	408	Request: CANCEL sip:172.16.119.4
2191	49.904757361	172.16.119.4	172.16.119.3	SIP/SDP	842	Request: INVITE sip:172.16.119.3
2192	49.911428937	172.16.119.3	172.16.119.4	SIP	430	Status: 100 Trying
2193	50.208022530	172.16.119.3	172.16.119.4	SIP	465	Status: 180 Ringing
2202	53.448283736	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2203	53.450991310	172.16.119.4	172.16.119.3	SIP	433	Request: ACK sip:172.16.119.3:5060
2254	53.948220693	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2355	54.947871114	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2540	56.947751381	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2697	58.407604600	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2699	58.578095694	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2700	58.579825755	172.16.119.4	172.16.119.3	SIP	452	Status: 481 Transaction does not exist
2701	58.908077009	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2702	59.077867358	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2705	59.908175992	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2706	60.078260776	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2709	61.908355385	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2710	61.910673860	172.16.119.3	172.16.119.4	SIP	428	Status: 200 OK
2711	62.077733958	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2712	62.078875525	172.16.119.4	172.16.119.3	SIP	452	Status: 481 Transaction does not exist

Рисунок 81 – Пакеты, отфильтрованные по протоколу SIP в Wireshark.

Установление аудио/видео сессии

Анализ участвовавших в соединении запросов и ответов SIP:

- определить идентификатор *Public User Identity* вызывающего пользователя;
(Зарегистрированный идентификатор *Public User Identity* вызывающего пользователя передается в заголовке *From* запроса *INVITE*.)
SIP from address User Part: popov.i
SIP from address Host Part: ngn.lab
SIP from tag: 1004
- определить идентификатор *Public User Identity* вызываемого пользователя;
(Зарегистрированный идентификатор *Public User Identity* вызываемого пользователя передается в заголовке *To* запроса *INVITE*.)
SIP to address User Part: ivanov.a
SIP to address Host Part: ngn.lab

- определить Идентификатор сессии;
(Передается в заголовке *Call-ID* запроса *INVITE*.)
Call-ID: efc835748287646508ced60bb3aeb496@172.16.119.9

- определить заголовок, в котором передается название терминала пользователя (вызываемого, вызывающего);
(Заголовок *User-Agent* запроса *INVITE* и *Server* ответа *200 OK*.)
User-Agent: Fokus MONSTER Version: 0.9.13

- определить длительность фазы установления соединения, фазы разговора, используя данные о времени отправки пакетов; (предполагается, что задержка прохождения пакетов по сети нулевая) (Рисунок 82);

(Фаза установления разговора: вычесть из времени отправки сообщения *ACK* - 9.920776168 время отправки сообщения *INVITE* - 3.981648665).

15	9.920776168	172.16.119.9	172.16.117.22	SIP	535	Request: ACK sip:ivanov.a@172.16.119.10:5060
4	3.981648665	172.16.119.9	172.16.117.22	SIP/SDP	767	Request: INVITE sip:ivanov.a@ngn.lab

Результат: 5,946556448.

- определить параметры мультимедийной сессии: параметры передачи речи (используемый кодек, номер порта для обработки медиаинформации на стороне вызывающего пользователя, номер порта для обработки медиаинформации на стороне вызываемого пользователя).

(Параметры мультимедийной сессии содержатся в теле сообщений *INVITE* и *200OK* в формате протокола *SDP*. Для просмотра тела сообщения следует в окне детального просмотра раскрыть строку *Message Body* (нажатием на кнопку «+» сбоку), затем раскрыть строку *Session Description Protocol*.

Строка тела сообщения «*Media Description, Name and Address*» имеет формат: тип передаваемой информации (аудио или видео); номер порта для обработки медиаинформации; транспортный протокол для передачи медиаинформации; поддерживаемые кодеки (кодируются числами, каждому типу кодека соответствует определенное число, например, 3 – кодек *GSM*); дополнительные параметры (также кодируются числами).

Используемый кодек: кодек, указанный в строке «*Media Description, Name and Address*» тела сообщения *200OK*. (см. 6 на Рисунок 82.)

Номер порта для обработки медиаинформации:

- на стороне вызывающего абонента: номер порта в строке «*Media Description, Name and Address*» в *SDP*-теле сообщения *INVITE*;

- на стороне вызываемого абонента: номер порта в строке «*Media Description, Name and Address*» в *SDP*-теле сообщения *200OK* (см. 5 на Рисунок 82).

Параметры мультимедийной сессии содержатся в теле сообщений *INVITE* и *200OK*.

ИСПОЛЬЗУЕМЫЙ КОДЕК: кодек, указанный в строке «*Media Description, Name and Address*» тела сообщения *200OK*:

Media Description, name and address (m): audio 23004 RTP/AVP 0 8 14 101

НОМЕР ПОРТА ДЛЯ ОБРАБОТКИ МЕДИАИНФОРМАЦИИ:

на стороне вызывающего абонента: номер порта в строке

Media Description, name and address (m): audio 23002 RTP/AVP 0 101

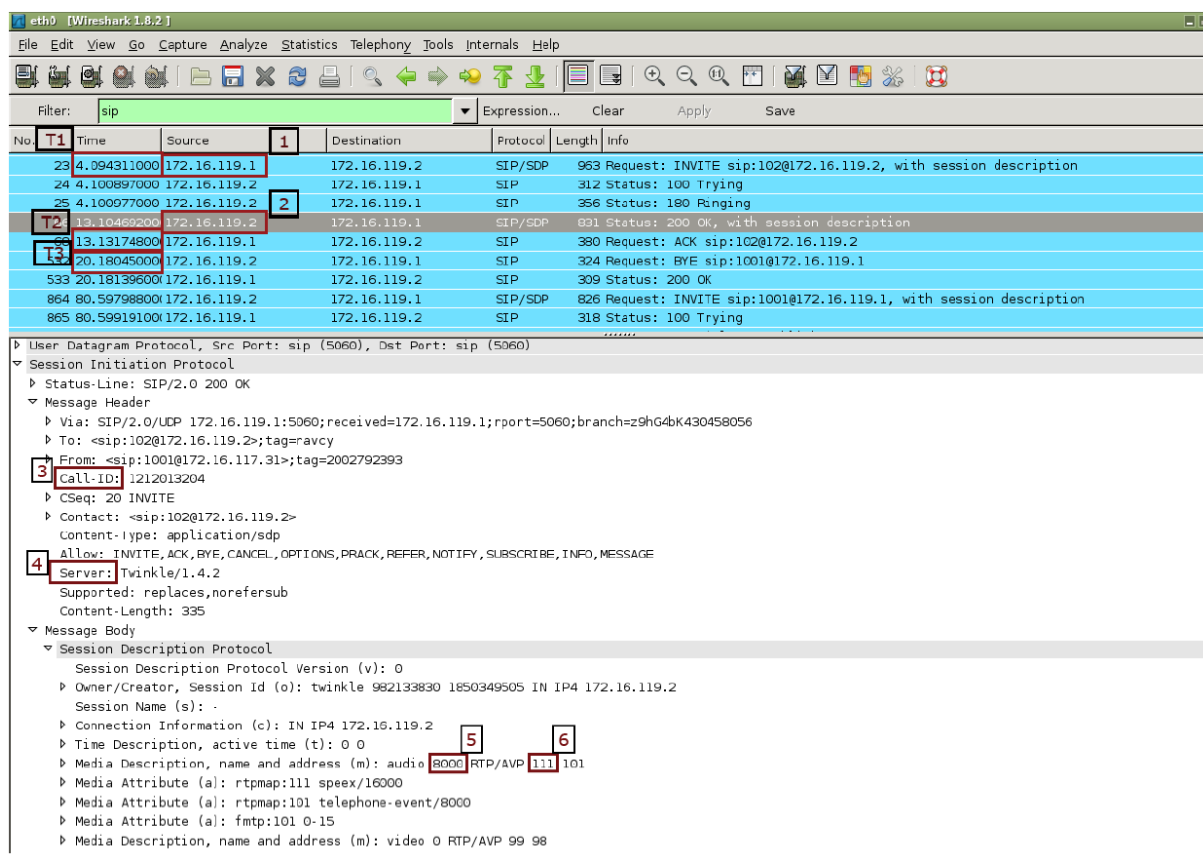


Рисунок 82 – Окно Wireshark с сигнальной информацией вызова

Услуга Chat

Осуществить обмен текстовыми сообщениями в режиме реального времени (чат) между пользователем РМ 1 и пользователем РМ 2.

- Определить элементы сети IMS, участвующие в процессе реализации услуги, по сигнальной информации, собранной с помощью программы Wireshark локально и на сервере (используйте ярлык «Файлы сигнальной информации»).

Два IMS-терминала, P-CSCF, S-CSCF.

- Определить сообщения SIP (запросы и ответы), отправленные для установления сессии, по сигнальной информации, собранной с помощью программы Wireshark.

Для установления сессии отправляется запрос INVITE, в ответ приходит 200 OK. После отправки ACK текстовая сессия считается установленной.

- Проанализировать участвовавшие в соединении запросы и ответы протокола SIP (составить отчет);
- определить параметры мультимедийной сессии;

(Параметры мультимедийной сессии содержатся в теле сообщений INVITE и 200OK в формате протокола SDP).

31	47.201664323	172.16.119.9	172.16.117.22	SIP	460	Request: MESSAGE sip:ivanov.a@ngn.lab (text/plain)
32	47.222571820	172.16.117.22	172.16.119.9	SIP	373	Status: 200 OK
54	65.667461569	172.16.117.22	172.16.119.9	SIP	942	Request: MESSAGE sip:rostov.m@172.16.119.9:5060 (text/plain)
56	65.677043523	172.16.119.9	172.16.117.22	SIP	606	Status: 200 OK

- определить протокол, используемый для передачи тестовых сообщений.

Протокол MSRP.

Услуга Instant message

Отправить мгновенное сообщение от пользователя РМ 1 к пользователю РМ 2.

- Определить элементы сети IMS, участвующие в процессе реализации услуги, по сигнальной информации, собранной с помощью программы Wireshark локально и на сервере (используйте ярлык «Файлы сигнальной информации»).

Два IMS-терминала, P-CSCF, S-CSCF.

Проанализировать участвовавших в соединении запросов и ответов протокола SIP (составить отчет);

- определить и проанализировать сообщения SIP (запросы и ответы), отправленные при передаче мгновенного сообщения, по сигнальной информации, собранной с помощью программы Wireshark;

Для передачи мгновенного сообщения передается сообщение MESSAGE протокола SIP, в ответ приходит 200 OK.

- определить заголовок, содержащий информацию о типе передаваемых данных; Заголовок Content-type сообщения MESSAGE.

- проанализировать тело сообщения, отправленного для передачи мгновенного сообщения.

Тело сообщения MESSAGE содержит отправленное текстовое сообщение.

Session Initiation Protocol (MESSAGE)

Request-Line: MESSAGE sip:rostov.m@172.16.119.9:5060 SIP/2.0

Message Header

Call-ID: 1b42c45af24f90aec95816fa6fc04af@172.16.119.10

CSeq: 3 MESSAGE

From: <sip:ivanov.a@ngn.lab>;tag=1004

To: <sip:popov.i@ngn.lab>

Via: SIP/2.0/UDP 172.16.117.22:4060;branch=z9hG4bKa58d.808d20b5.0

Via: SIP/2.0/UDP 172.16.117.24:6060;received=172.16.117.24; rport=6060; branch=z9hG4bKa58d.ce9bcb6.0

Via: SIP/2.0/UDP 172.16.117.24:6060;branch=z9hG4bKa58d.be9bcb6.0

Via: SIP/2.0/UDP 172.16.117.22:4060;branch=z9hG4bKa58d.708d20b5.0

Via: SIP/2.0/UDP 172.16.119.10:5060;rport=5060;branch=z9hG4bK7fe9ee7af021472c7edcca7efcd38e41373036

Max-Forwards: 13

Content-Type: text/plain

User-Agent: Fokus MONSTER Version: 0.9.13

Content-Length: 3

P-Asserted-Identity: <sip:ivanov.a@ngn.lab>

SIP PAI Address: sip:ivanov.a@ngn.lab

P-Charging-Vector: icid-value="P-CSCFabcd590ae8c5000000c1";icid-generated-at=172.16.117.22;orig-ioi="ngn.lab"

P-Called-Party-ID: <sip:popov.i@ngn.lab>

Message Body

Line-based text data: text/plain

bye

Файловая сессия

Отправить любой файл от пользователя РМ 1 к пользователю РМ 2.

- Определить элементы сети IMS, участвующие в процессе передачи файла, по сигнальной информации, собранной с помощью программы Wireshark;

Два IMS-терминала, P-CSCF, S-CSCF

- Проанализировать участвовавшие в соединении запросы и ответы SIP (составить отчет);

```

1004 5.510232408 172.16.119.9 172.16.117.22 SIP/SDP 1023 Request: INVITE sip:ivanov.a@172.16.119.10:5060, in-dialog |
1005 5.511442296 172.16.117.22 172.16.119.9 SIP 624 Status: 100 trying -- your call is important to us |
1017 5.563714009 172.16.117.22 172.16.119.9 SIP/SDP 775 Status: 200 OK |
1018 5.571192159 172.16.119.9 172.16.117.22 SIP 531 Request: ACK sip:ivanov.a@172.16.119.10:5060 |
2518 12.131685756 172.16.119.9 172.16.117.22 SIP/SDP 1388 Request: INVITE sip:ivanov.a@172.16.119.10:5060, in-dialog |
2519 12.132966505 172.16.117.22 172.16.119.9 SIP 624 Status: 100 trying -- your call is important to us |

```

- определить сообщения SIP (запросы и ответы), отправленные при передаче файла, по сигнальной информации, собранной с помощью программы Wireshark;

Для установления сессии отправляется запрос INVITE, в ответ приходит 200 OK. После отправки ACK текстовая сессия считается установленной.

- определить протокол, по которому осуществляется передача файла; протокол MSRP.

- проанализировать тела сообщений, отправленные при передаче файла.

Параметры мультимедийной сессии содержатся в теле сообщений INVITE и 200OK в формате протокола SDP.

Session Description Protocol

Session Description Protocol Version (v): 0

Owner/Creator, Session Id (o): popov.i 3702876729 3702876744 IN IP4 172.16.119.9

Session Name (s): A Funky MONSTER Stream

Time Description, active time (t): 0 0

Media Description, name and address (m): audio 23002 RTP/AVP 0 101

Connection Information (c): IN IP4 172.16.119.9

Media Attribute (a): rtpmap:0 PCMU/8000

Media Attribute (a): rtpmap:101 telephone-event/8000

Media Description, name and address (m): video 23004 RTP/AVP 34

Connection Information (c): IN IP4 172.16.119.9

Media Attribute (a): rtpmap:34 H263/90000

*Media Description, name and address (m): message 7394 TCP/MSRP **

Connection Information (c): IN IP4 172.16.119.9

Media Attribute (a): accept-types:text/plain

Media Attribute (a): path:msrp://172.16.119.9:7394/977a33634018057d;tcp

*Media Description, name and address (m): message 7394 TCP/MSRP **

Connection Information (c): IN IP4 172.16.119.9

Media Attribute (a): file-selector:name:"client-ims-core.jar" type:application/octet-stream size:1335683 hash:sha-1:5A:02:54:F1:DC:06:3C:0F:DA:57:62:9D:6D:01:86:C8:6D:D9:E2:2B

Media Attribute (a): file-range:1-1335683

Media Attribute (a): disposition:attachment

Media Attribute (a): accept-types:application/octet-stream

Media Attribute (a): path:msrp://172.16.119.9:7394/be1677c4964d3340;tcp

Media Attribute (a): sendonly

Лабораторная работа №3 «Мультимедийные сессии»

Регистрация и совершение вызова

Проходим процедуру регистрации в сети IMS и подтвердить аккаунт в программе IMS-клиент Monster (Рисунок 83, Рисунок 84). Необходимо заполнить данные пользователя (имя и

секретный ключ), а также изменить IMSU, после чего уже приступить к подтверждению профиля в программе IMS-клиент Monster (Рисунок 85).

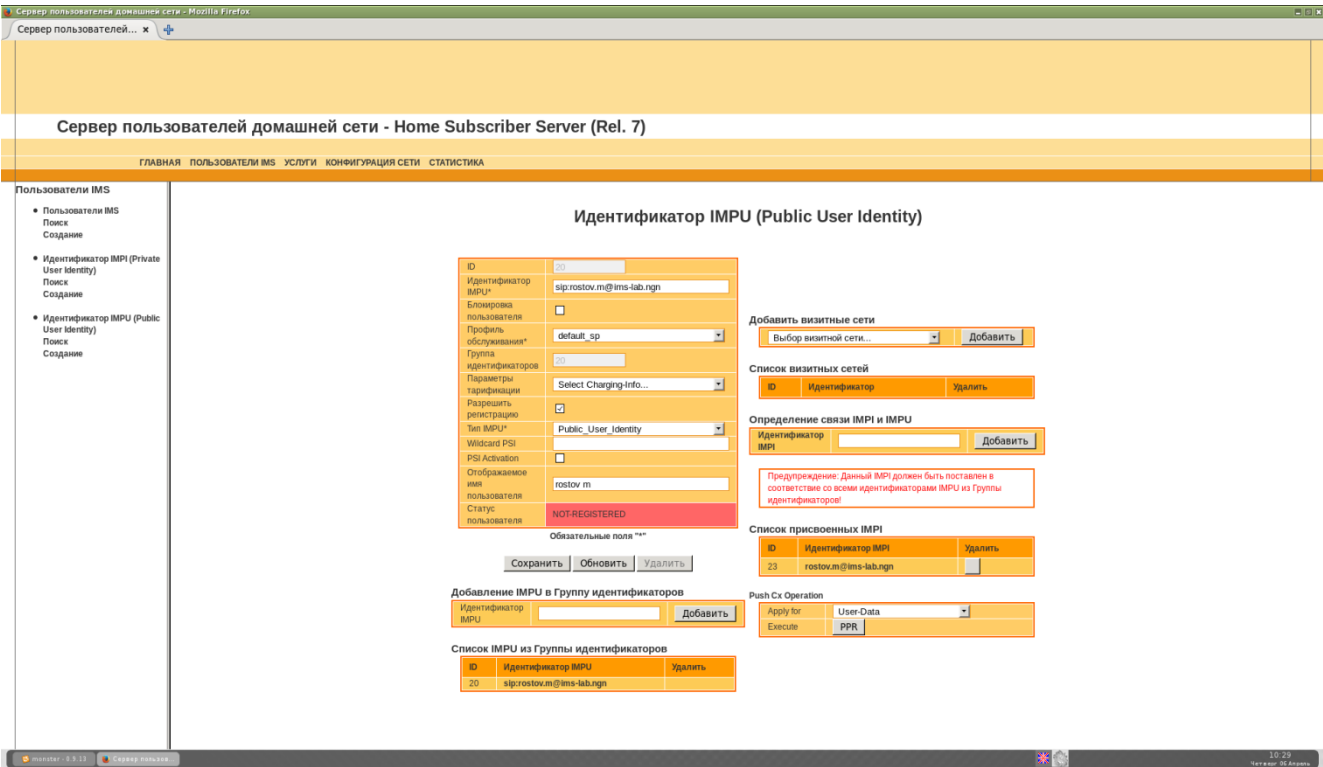


Рисунок 83 – Процедура регистрации пользователя в сети IMS

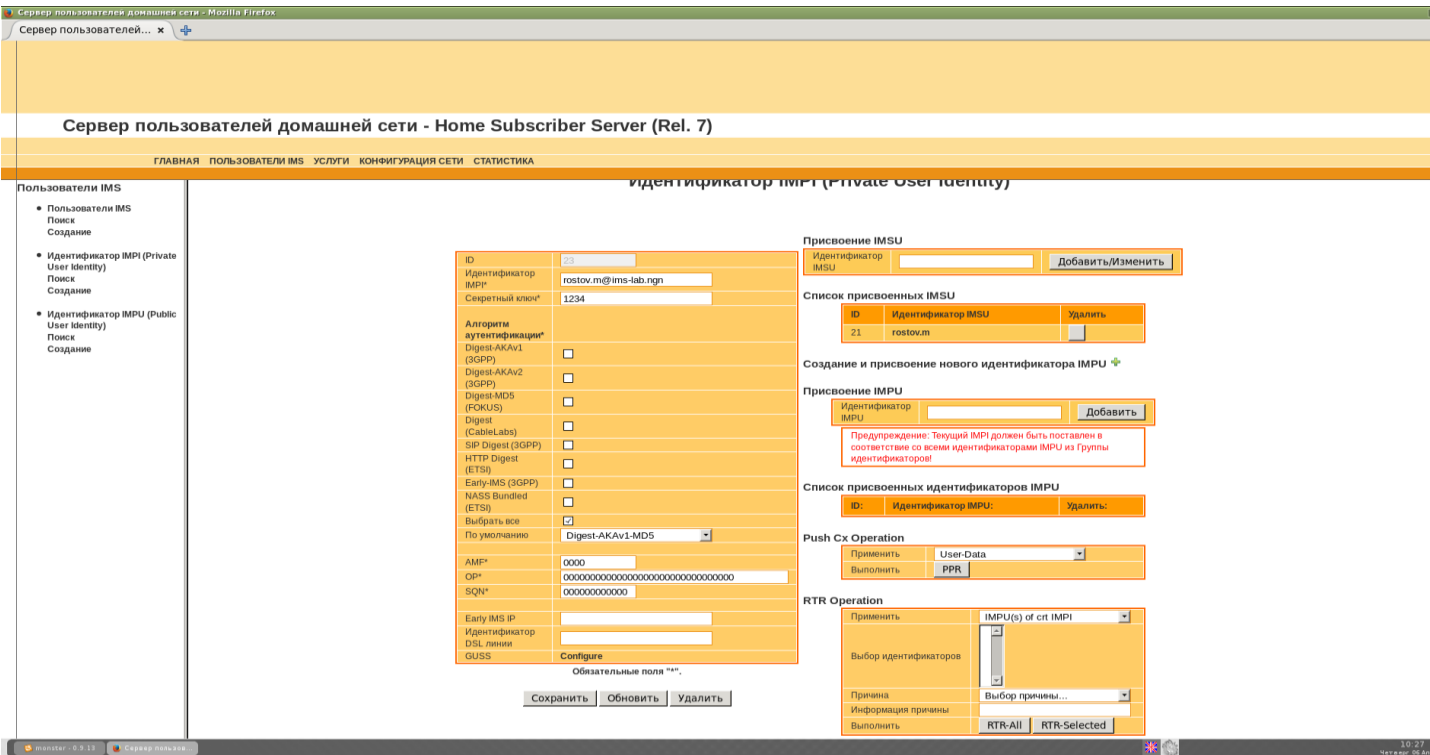


Рисунок 84 – Процедура регистрации пользователя в сети IMS



Рисунок 85 – Подтверждение аккаунта в программе Monster IMS и конфигурация

Далее требуется установить мультимедийную сессии между зарегистрированными пользователями IMS, находящимися в домашних сетях. Затем подключить Wireshark, запускающийся с рабочего стола машины, где необходимо выбрать сетевой интерфейс eth0.

Аудиосессия с передачей файлов

Алгоритм

Включение *Wireshark* и выбор интерфейса *eth0*.

Включение и регистрация пользователей в *IMS Monster* на двух разных машинах.

Звонок с одной машины на другую в программе *IMS Monster*. (Номер для звонка представляет собой обрезанный по примеру SIP логин другого пользователя, например: sip:ivanov.a@ngn.lab, в этом случае номер для звонка это *ivanov.a*).

В интерфейсе звонка выбрать иконку *Start Chat* и с ее помощью открыть его.

В открывшемся интерфейсе чата выбрать пункт *Send File* и в открывшемся меню выбрать файл, который необходимо отправить (лучшим вариантом будет сделать скриншот и после отправить его).

На машине получателя подтвердить получение файла, сохранить его и дать отбой.

Остановить перехват логов *Wireshark*, сохранить их и открыть.

В логах необходимо задать фильтрацию по протоколу *SIP*.

Определить, какие логи отвечают за установление аудиосессии и какие за отправку файлов, для аудиосессии - стандартные SIP

66	51.562737816	172.16.119.10	172.16.117.22	SIP/SDP	772 Request: INVITE sip:rostov.m@ngn.lab
67	51.563505409	172.16.117.22	172.16.119.10	SIP	600 Status: 100 trying -- your call is important to us
68	51.640434857	172.16.117.22	172.16.119.10	SIP	587 Status: 180 Ringing
69	54.009586480	172.16.117.22	172.16.119.10	UDP	60 4060 → 5060 Len=2
70	54.312358632	172.16.117.22	172.16.119.10	SIP/SDP	794 Status: 200 OK
71	54.320964031	172.16.119.10	172.16.117.22	SIP	536 Request: ACK sip:rostov.m@172.16.119.9:5060
72	54.335585208	172.16.119.9	172.16.119.10	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3FD72E17, Seq=21571, Time=2198554924, Mark
73	54.335618410	172.16.119.10	172.16.119.9	ICMP	242 Destination unreachable (Port unreachable)
74	54.348373991	172.16.119.9	172.16.119.10	RTP	214 PT=ITU-T G.711 PCMU, SSRC=0x3FD72E17, Seq=21572, Time=2198555084

Для передачи файла фильтрация по *MSRP*.

No.	Time	Source	Destination	Protocol	Length	Info
2289	75.845692225	172.16.119.10	172.16.119.9	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x8EC839BF, Seq=15657, Time=2368652848
2290	75.846608101	172.16.119.9	172.16.119.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3FD72E17, Seq=22647, Time=2198727084
2291	75.852691969	172.16.119.10	172.16.119.9	MSRP	1514	Request: SEND Transaction ID: a077cb889eec560
2292	75.852708047	172.16.119.10	172.16.119.9	TCP	993	7394 → 7394 [PSH, ACK] Seq=13322 Ack=876 Win=34560 Len=927 TSval=2014060 TSecr=507182
2293	75.853359336	172.16.119.9	172.16.119.10	TCP	66	7394 → 7394 [ACK] Seq=876 Ack=14249 Win=57472 Len=0 TSval=507184 TSecr=2014060
2294	75.857141939	172.16.119.9	172.16.119.10	MSRP	239	Response: 200 Success Transaction ID: a077cb889eec560
2295	75.863416056	172.16.119.10	172.16.119.9	MSRP	1514	Request: SEND Transaction ID: a249d028bf37098a
2296	75.863431487	172.16.119.10	172.16.119.9	TCP	995	7394 → 7394 [PSH, ACK] Seq=15697 Ack=1049 Win=35712 Len=929 TSval=2014062 TSecr=507185
2297	75.864095080	172.16.119.9	172.16.119.10	TCP	66	7394 → 7394 [ACK] Seq=1049 Ack=16626 Win=62336 Len=0 TSval=507186 TSecr=2014062
2298	75.864672809	172.16.119.9	172.16.119.10	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3FD72E17, Seq=22648, Time=2198727244

Составляем диаграмму с помощью Wireshark - пункт меню Statistics - Flow Graph с фильтрацией по протоколу SIP (Show - allpackets).

Аудиосессия с передачей мгновенного сообщения Instant message.

Алгоритм

Включение Wireshark и выбор интерфейса eth0.

Включение и регистрация пользователей в IMS Monster на двух разных машинах.

Звонок с одной машины на другую в программе IMS Monster. (Номер для звонка представляет собой обрезанный по примеру SIP логин другого пользователя, например: sip:ivanov.a@ngn.lab, в этом случае номер для звонка это ivanov.a)

Выбираем вкладку Messages жмем new и указываем адрес другого пользователя в соответствии с заданием в виде sip:ivanov.a@ngn.lab

Отправляем сообщение и завершаем сеанс связи.

Остановить перехват логов Wireshark, сохранить их и открыть.

В логах необходимо задать фильтрацию по протоколу SIP.

Логом отправки сообщения является лог строка с указателем MESSAGE, копируем данное сообщение в отчет.

Составляем диаграмму с помощью Wireshark - пункт меню Statistics - Flow Graph с фильтрацией по протоколу SIP (Show – allpackets) (Рисунок 86).



Рисунок 86 – Диаграмма аудиосессии с передачей мгновенного сообщения Instant message

Видеосессия и передача текстовых сообщений чата (Chat).

Алгоритм

Включение Wireshark и выбор интерфейса eth0.

Включение и регистрация пользователей в IMS Monster на двух разных машинах.

Добавляем третьего пользователя в друзья, чтобы была возможность начать чат.

Звонок с одной машины на другую в программе IMS Monster. (Номер для звонка представляет собой обрезанный по примеру SIP логин другого пользователя, например:

sip:ivanov.a@ngn.lab, в этом случае номер для звонка это *ivanov.a*)

Ждем когда третий пользователь начнет чат с помощью выбора пользователя из окна «Друзья».

Пишем что-нибудь в чат друг другу.

Отправляем сообщение и завершаем сеанс связи.

Останавливаем перехват логов Wireshark, сохраняем их и открываем.

В логах необходимо задать фильтрацию по протоколу *SIP*.

Проводим разбор и разграничиваем чат и видеосессию (две разные сессии для каждого адреса и команды INVITE).

Вносим эту информацию в отчет с соответствующими комментариями.

Составляем диаграмму с помощью *Wireshark* - пункт меню *Statistics - Flow Graph* с фильтрацией по протоколу *SIP (Show - allpackets)* (Рисунок 87).



Рисунок 87 – Диаграмма видеосессии и передачи текстовых сообщений чата

Лабораторная работа №4 «Дополнительные услуги»

Регистрация и совершение вызова

Проходим процедуру регистрации в сети IMS и подтвердить аккаунт в программе IMS-клиент Monster (Рисунок 88, Рисунок 89). Необходимо заполнить данные пользователя (имя и секретный ключ), а также изменить IMSU, после чего уже приступить к подтверждению профиля в программе IMS-клиент Monster (Рисунок 90).

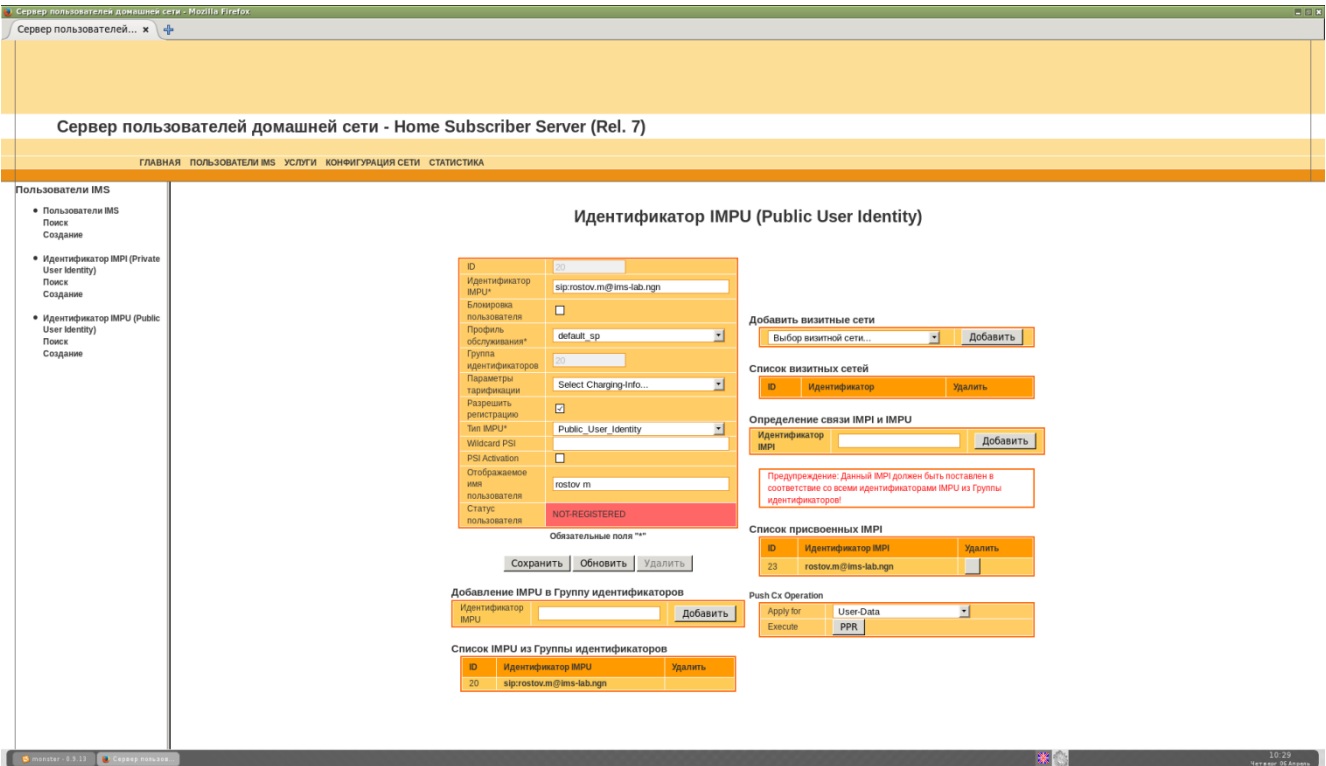


Рисунок 88 – Процедура регистрации пользователя в сети IMS

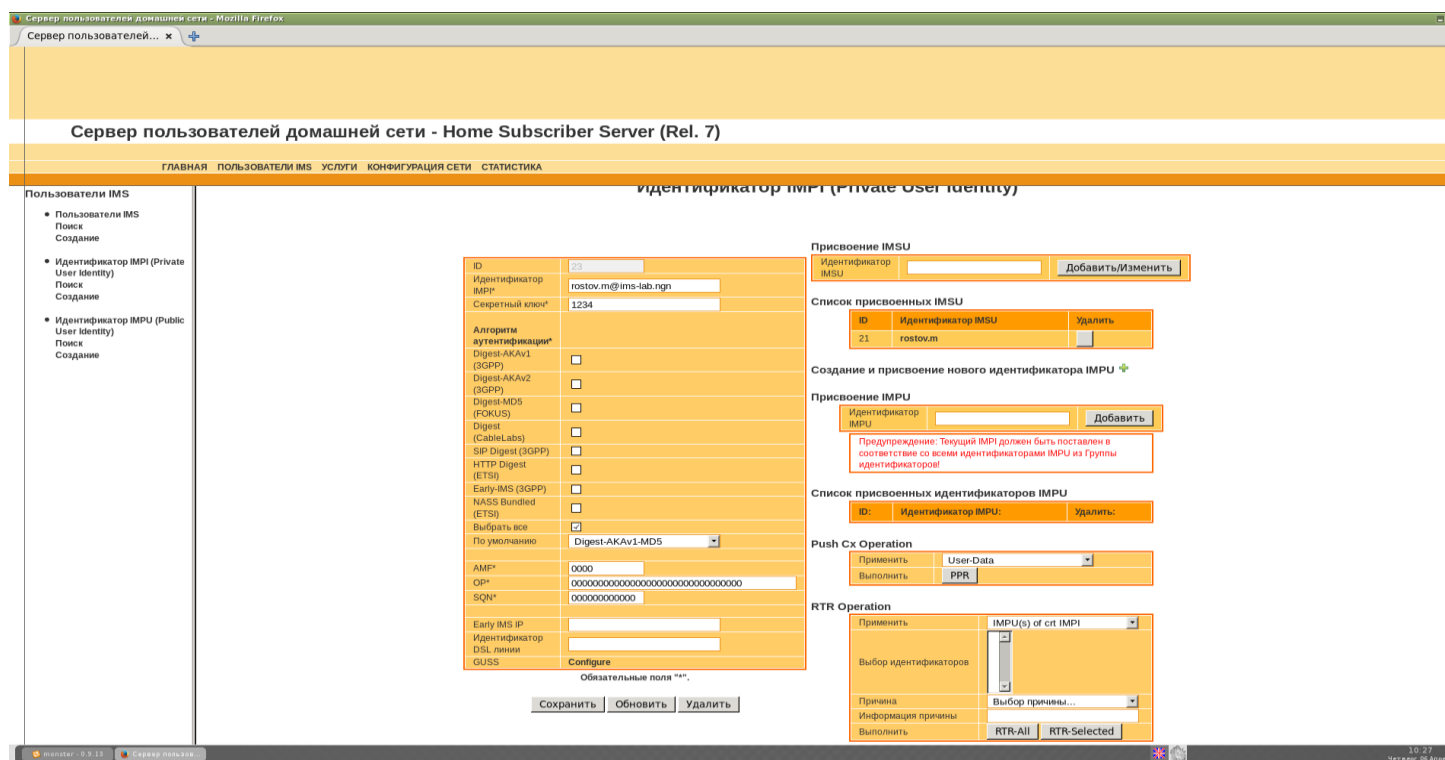


Рисунок 89 – Процедура регистрации пользователя в сети IMS



Рисунок 90 – Подтверждение аккаунта в программе Monster IMS и конфигурация

Возможны два варианта процедуры регистрации: с аутентификацией и без аутентификации. В случае если пользователь впервые регистрируется в сети IMS, ему необходимо пройти

аутентификацию (Рисунок 91). При повторной регистрации аутентификация пользователя не требуется. Прежде чем начать регистрацию оборудование пользователя (UE) осуществляет поиск точки доступа в сеть IMS (P-CSCF).

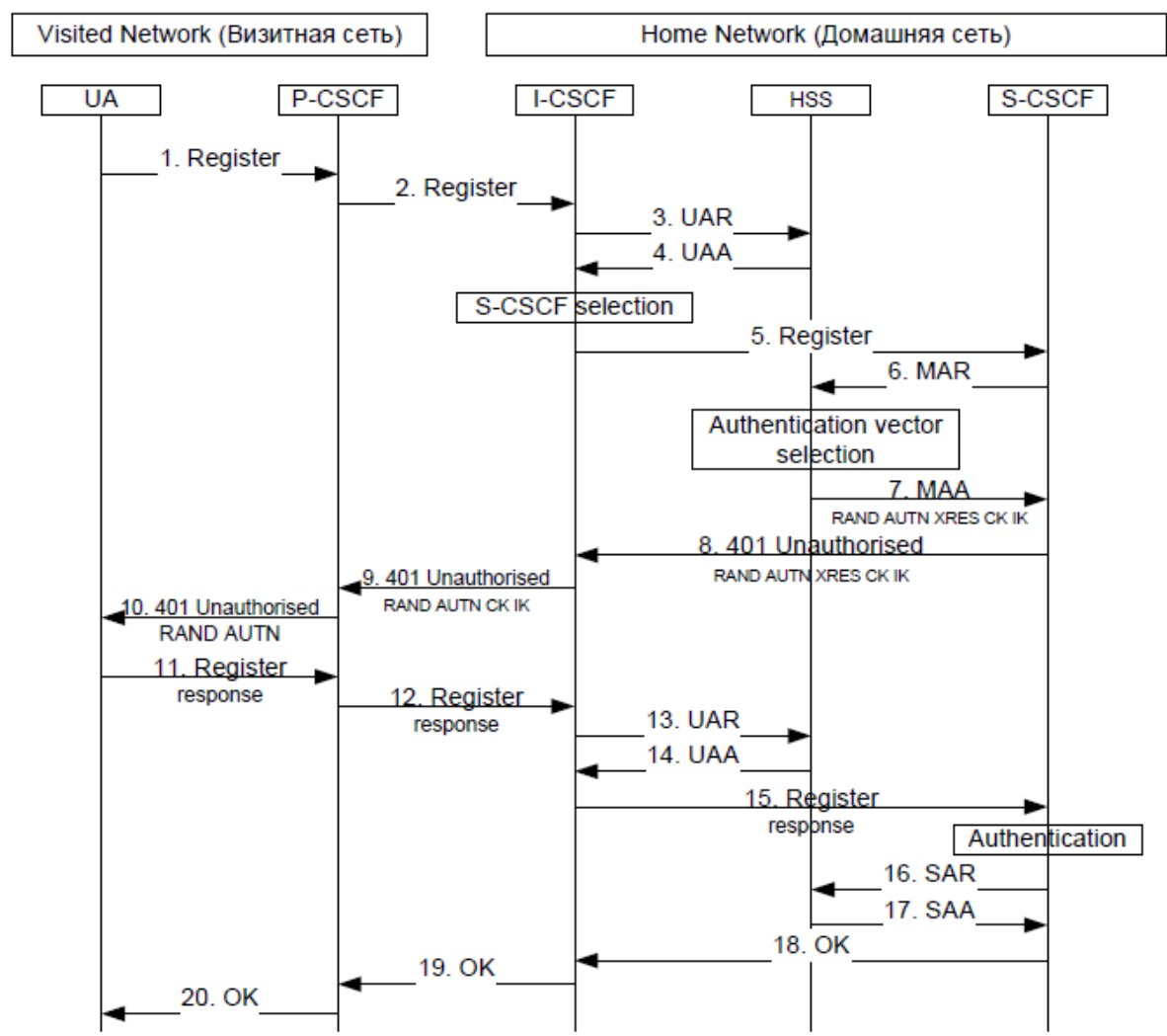


Рисунок 91 – Процедура регистрации пользователя в сети IMS

Далее требуется установить мультимедийную сессии между зарегистрированными пользователями IMS, находящимися в домашних сетях. IP-адрес рабочего места А будет 172.16.119.3. IP-адрес рабочего места В будет 172.16.119.4.

Необходимо пройти регистрацию в программе Twinkle (Рисунок 92, Рисунок 93, Рисунок 94), заполняя данные в каждом из полей, в соответствии с указанными там данными и IP адресом рабочего места.

Запускаем Wireshark. Совершаем звонок в программе Twinkle (Рисунок 95, Рисунок 96). Осуществляем фильтрацию по проколу SIP в Wireshark.

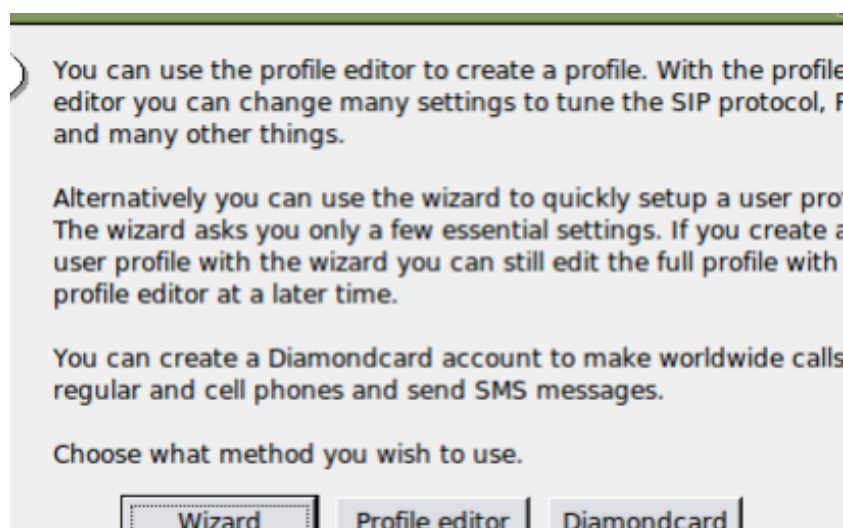


Рисунок 92 – Запуск мастера в программе Twinkle

A screenshot of a dialog box titled 'Twinkle - User profile wizard: 206'. It contains several input fields and a dropdown menu. The fields are labeled: 'SIP service provider:' (dropdown menu showing 'Other'), 'Your name:', 'User name*:', 'Domain*:', 'Authentication name:', 'Password:', 'SIP proxy:', and 'STUN server:'. The values entered are: 'Other', '206', '206', '172.16.117.233', '206', an empty field, '172.16.117.233', and an empty field. At the bottom right, there are 'OK' and 'Cancel' buttons.

Рисунок 93 – Процедура регистрации пользователя в программе Twinkle

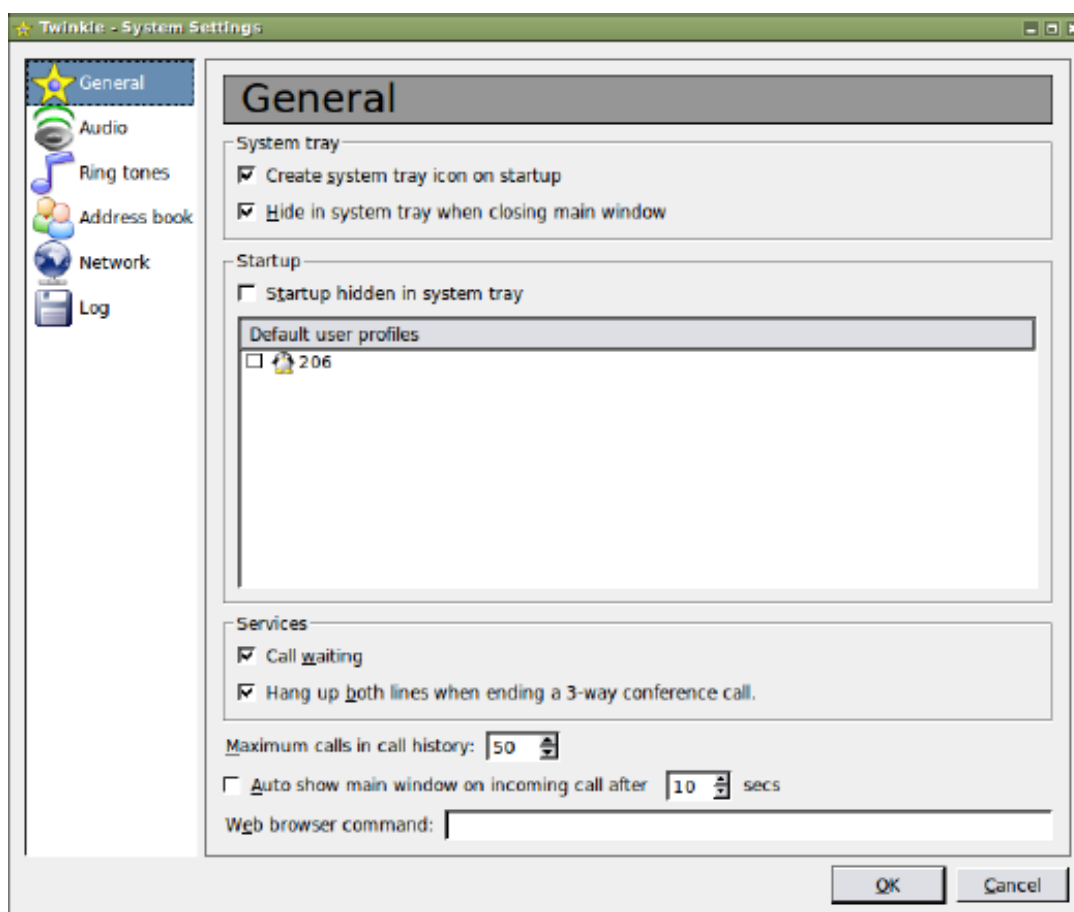


Рисунок 94 – Процедура регистрации пользователя в программе Twinkle

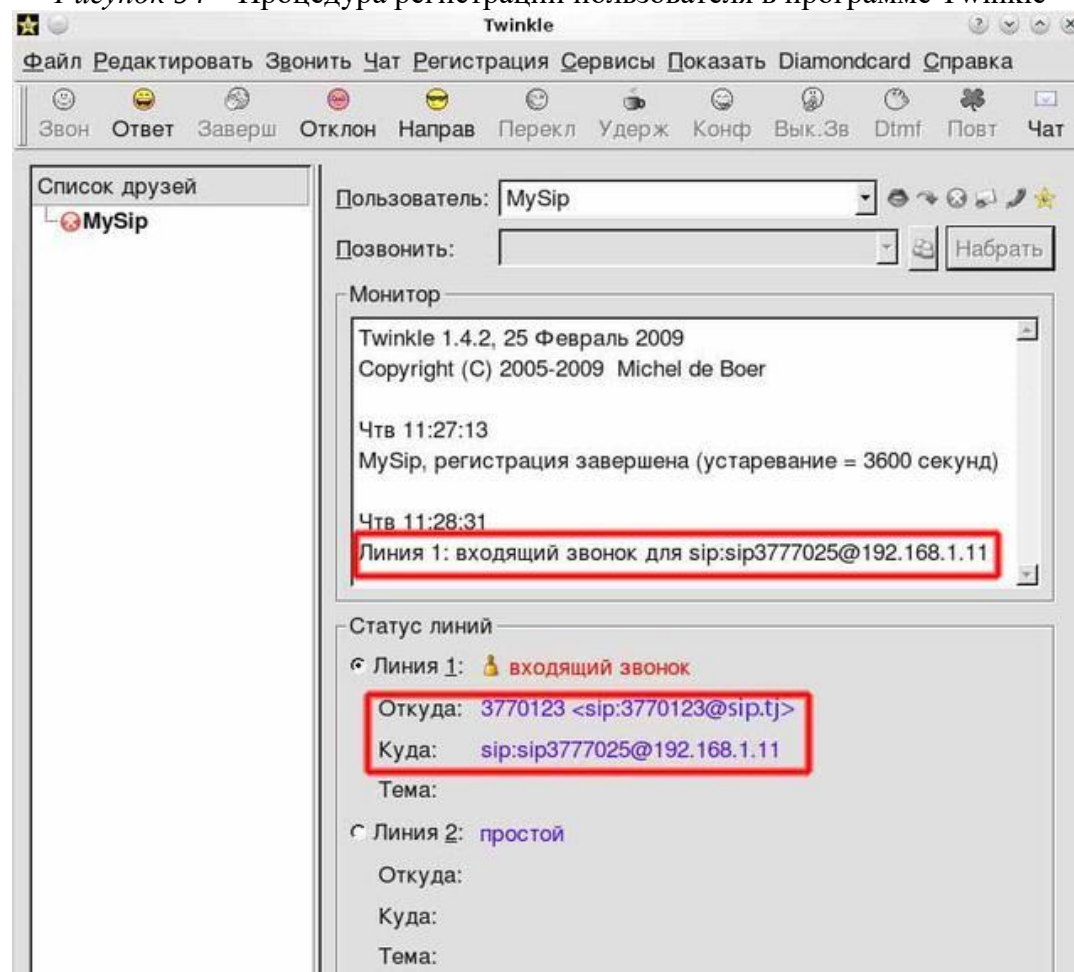


Рисунок 95 – Звонок в программе Twinkle

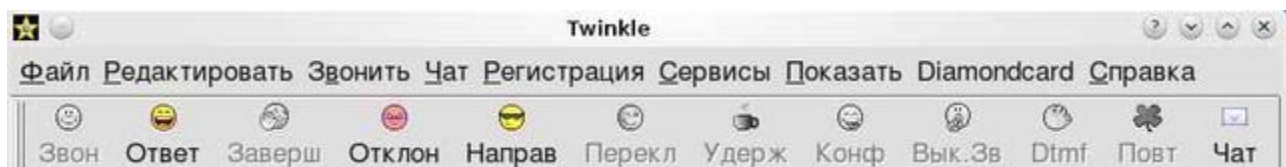


Рисунок 96 –Процедура принятия вызова в программе Twinkle

Пользователь *User A* инициирует вызов к пользователю *User B*. Терминальное оборудование пользователя *User A* отправляет сообщение *INVITE* протокола *SIP* для запроса установления мультимедийной сессии с пользователем *User B*, содержащее описание сессии в формате *SDP* для передачи данных от *User B* к *User A*. *P-CSCFA* принимает запрос *INVITE*, заменяет в запросе *INVITE* заголовок *P-Preferred-Identity* на заголовок *P-Asserted-Identity*, содержащий зарегистрированный идентификатор *PuUI* вызывающего пользователя, добавляет в заголовок *Route* свой адрес и отправляет запрос к функциональному объекту *S-CSCFA*. К оборудованию вызываемого пользователя *P-CSCFA* отправляет ответ с кодом *100 (Trying)*. Этот ответ информирует терминал о том, что запрос *INVITE* был получен, и прокси-сервер выполняет маршрутизацию запроса к месту назначения. *S-CSCFA* на основании идентификатора пользователя *User B*, содержащегося в запросе *INVITE*, определяет входную точку в домашнюю сеть вызываемого пользователя *I-CSCFB*. После чего отправляет запрос *INVITE* к *I-CSCFB*, а к *P-CSCFA* ответ *100 (Trying)*. Ниже представлен примерный листинг из программы *Wireshark*:

2187	49.404434830	172.16.119.4	172.16.119.3	SIP/SDP	842	Request: INVITE sip:172.16.119.3
2189	49.526995695	172.16.119.3	172.16.119.4	SIP	408	Request: CANCEL sip:172.16.119.4
2191	49.904757361	172.16.119.4	172.16.119.3	SIP/SDP	842	Request: INVITE sip:172.16.119.3
2192	49.911428937	172.16.119.3	172.16.119.4	SIP	430	Status: 100 Trying
2193	50.208022530	172.16.119.3	172.16.119.4	SIP	465	Status: 180 Ringing
2202	53.448283736	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2203	53.450991310	172.16.119.4	172.16.119.3	SIP	433	Request: ACK sip:172.16.119.3:5060
2254	53.948220693	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2355	54.947871114	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2540	56.947751381	172.16.119.3	172.16.119.4	SIP/SDP	711	Status: 200 OK
2697	58.407604600	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2699	58.578095694	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2700	58.579825755	172.16.119.4	172.16.119.3	SIP	452	Status: 481 Transaction does not exist
2701	58.908077009	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2702	59.077867358	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2705	59.908175992	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2706	60.078260776	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2709	61.908355385	172.16.119.4	172.16.119.3	SIP	433	Request: BYE sip:172.16.119.3:5060
2710	61.910673860	172.16.119.3	172.16.119.4	SIP	428	Status: 200 OK
2711	62.077733958	172.16.119.3	172.16.119.4	SIP	433	Request: BYE sip:172.16.119.4:5060
2712	62.078875525	172.16.119.4	172.16.119.3	SIP	452	Status: 481 Transaction does not exist

Чтобы определить IP-адрес вызывающего абонента и указать сообщение *SIP* и заголовок, в котором он содержится, необходимо найти строку 2187 и выбрать IP-адрес: **172.16.119.4**.

Чтобы определить IP-адрес вызываемого абонента и указать сообщение *SIP* и заголовок, в котором он содержится, нужно из строки 2202 выбрать IP-адрес: **172.16.119.3**.

Постановка вызова на удержание (Call Hold, CH)

Необходимо во время вызова нажать на кнопку «Удержание», находящуюся на панели задач *Twinkle* (Рисунок 97).

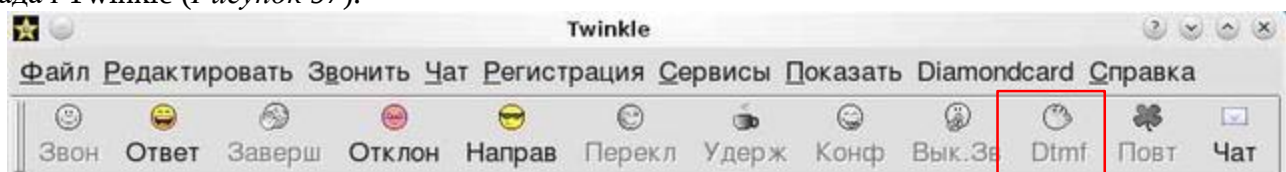


Рисунок 97 Процедура постановки вызова на удержание в программе Twinkle

Далее заходим в WireShark и анализируем полученные данные по протоколу SIP. Примерный листинг программы WireShark.

```
142 12.312015971 172.16.119.4 172.16.119.3 SIP/SDP 846 Request: INVITE sip:student3@172.16.119.3 |
143 12.315548117 172.16.119.3 172.16.119.4 SIP 332 Status: 100 Trying |
144 12.315629740 172.16.119.3 172.16.119.4 SIP 381 Status: 180 Ringing |
189 18.912131605 172.16.119.3 172.16.119.4 SIP/SDP 718 Status: 200 OK |
196 18.969650996 172.16.119.4 172.16.119.3 SIP 353 Request: ACK sip:student3@172.16.119.3 |
337 20.368646517 172.16.119.4 172.16.119.3 SIP/SDP 868 Request: INVITE sip:student3@172.16.119.3,
in-dialog |
339 20.370271350 172.16.119.3 172.16.119.4 SIP/SDP 730 Status: 200 OK |
343 20.398622891 172.16.119.4 172.16.119.3 SIP 353 Request: ACK sip:student3@172.16.119.3 |
356 23.529320957 172.16.119.4 172.16.119.3 SIP/SDP 856 Request: INVITE sip:student3@172.16.119.3,
in-dialog |
357 23.531202774 172.16.119.3 172.16.119.4 SIP/SDP 718 Status: 200 OK |
358 23.532701687 172.16.119.4 172.16.119.3 SIP 353 Request: ACK sip:student3@172.16.119.3 |
565 25.441548900 172.16.119.4 172.16.119.3 SIP 353 Request: BYE sip:student3@172.16.119.3 |
566 25.443096475 172.16.119.3 172.16.119.4 SIP 335 Status: 200 OK |
```

Чтобы определить запрос, осуществляющий постановку вызова на удержание, необходимо найти строку 337.

Запрос INVITE, отправленный во время уже установленного сеанса связи (второй по счету INVITE в сигнальных сообщениях конкретного вызова).

```
337 20.368646517 172.16.119.3 172.16.119.8 SIP/SDP 868 Request: INVITE sip:stu-
dent3@172.16.119.8, in-dialog |
```

Проанализировать полученную сигнальную информацию (составить отчет):

- определить запрос, осуществляющий постановку вызова на удержание, проанализировать параметры мультимедийного сеанса в этом запросе, определить их отличие от параметров мультимедийного сеанса в первом запросе INVITE;

Запрос INVITE, отправленный во время уже установленного сеанса связи (второй по счету INVITE в сигнальной информации вызова) со-держит новое описание сеанса связи, в котором указано о прекращении передачи медиаинформации (постановка на удержание). Описание сеанса связи в формате SDP содержится в теле запроса INVITE. Основное отличие: значение «0.0.0.0» в строке Connection information и/или наличие параметра sendonly

```
337 20.368646517 172.16.119.3 172.16.119.8 SIP/SDP 868 Request: INVITE sip:stu-
dent3@172.16.119.8, in-dialog |
```

Session Initiation Protocol (INVITE)

Message Body

Session Description Protocol

Media Attribute (a): sendonly

- определить запрос, снимающий вызов с удержания, проанализировать параметры мультимедийного сеанса в этом запросе, определить их отличие от параметров мультимедийного сеанса в первом запросе INVITE;

Запрос INVITE, отправленный после запроса постановки на удержание.

Запрос, снимающим вызов с удержания содержится в 356 строке листинга

Запрос INVITE, отправленный после запроса постановки на удержание.

```
356 23.529320957 172.16.119.3 172.16.119.8 SIP/SDP 856 Request: INVITE sip:stu-
dent3@172.16.119.8, in-dialog |
```

- Проанализировать параметры мультимедийного сеанса в запросе, снимающий вызов с удержания, определить их отличие от изначальных параметров мультимедийного сеанса

Основное отличие: наличие параметра sendonly(в данном листинге это будет 7303 строка, выделенная пунктир-точкой, в которой содержится данный параметр).

7303 306.694114907 172.16.119.10 172.16.119.8 SIP/SDP 865 Request: INVITE
sip:student8@172.16.119.8, in-dialog |

Session Initiation Protocol (INVITE)

Message Body

Session Description Protocol

Media Attribute (a): sendonly

- Определить время, в течение которого абонент находится на удержании.

Для расчета времени, в течение которого абонент находится на удержании, необходимо вычесть из времени отправки третьего сообщения ACK (в данном листинге это будет 358 строка, выделенная синей линией, где второй параметр – время выполнения):

358 23.532701687 172.16.119.3 172.16.119.8 SIP 353 Request: ACK sip:student3@172.16.119.8 |

(время: 23.532701687)

время отправки второго сообщения ACK (из строки 343, выделенной синей линией):

343 20.398622891 172.16.119.3 172.16.119.8 SIP 353 Request: ACK sip:student3@172.16.119.8 |

(время: 20.398622891):

23,5327 - 20,3986 = **3.1341**

Услуга «Не беспокоить» (Do not Disturb, DND)

Для активации услуги «Не беспокоить» необходимо в программе Twinkle перейти в меню «Сервисы» и выбрать пункт «Не беспокоить» (Рисунок 98).

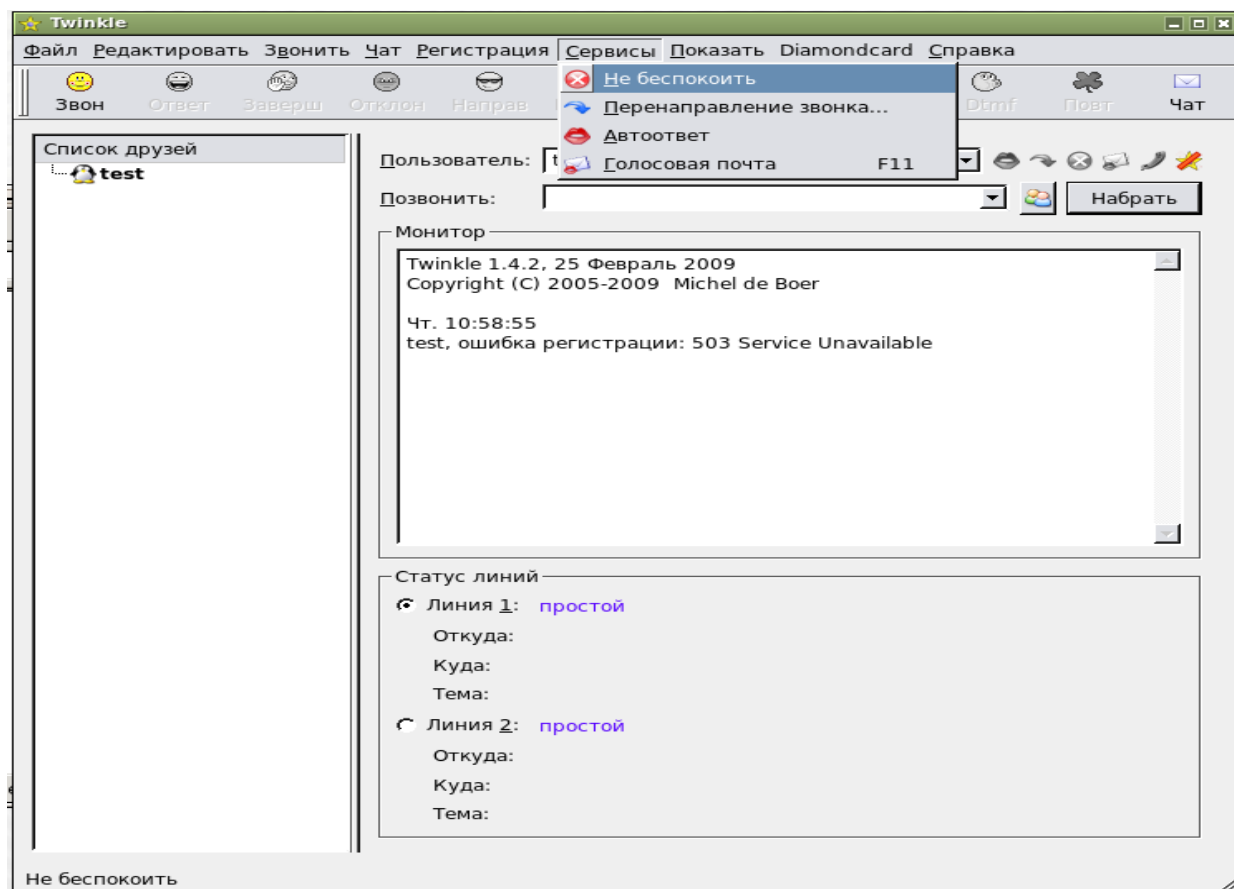


Рисунок 98 Процедура включения режима «Не беспокоить» в программе Twinkle

Если на телефоне активирована услуга «не беспокоить», то при поступлении входящего вызова он выдает информацию о том, что пользователь занят.

Порядок действий:

1. Активируем данную услугу «не беспокоить».
2. Осуществим вызов от Абонента А к Абоненту В.

3. Проанализировать полученную сигнальную информацию и составить отчет: определить окончательный ответ на запрос *INVITE*, и составить диаграмму обмена сообщениями SIP между всеми участниками сессии.

Ответ 480 Temporarily Unavailable или 486 Busy Here. В заголовке ответа CSeq указывается, на какой запрос был отправлен данный ответ.

Проанализировали участвовавшие в соединении запросы и ответы в программе WireShark.

Ниже представлен примерный листинг программы WireShark:

57	5.648873543	172.16.119.1	172.16.117.31	SIP/SDP	830	Request: INVITE
sip:1002@172.16.117.31						
58	5.651764727	172.16.117.31	172.16.119.1	SIP	495	Status: 100 Trying
59	5.704459008	172.16.117.31	172.16.119.1	SIP/SDP	838	Status: 200 OK
61	5.724526037	172.16.119.1	172.16.117.31	SIP	349	Request: ACK sip:1002@172.16.117.31:5060
769	16.266921416	172.16.117.31	172.16.119.1	SIP	455	Request: BYE sip:1001@172.16.119.1
770	16.269040160	172.16.119.1	172.16.117.31	SIP	337	Status: 200 OK
777	20.244417275	172.16.117.31	172.16.119.1	SIP/SDP	1100	Request: INVITE
sip:1001@172.16.119.1						
778	20.247003180	172.16.119.1	172.16.117.31	SIP	363	Status: 100 Trying
779	20.247240360	172.16.119.1	172.16.117.31	SIP	392	Status: 480 Temporarily Not Available
780	20.248021044	172.16.117.31	172.16.119.1	SIP	442	Request: ACK sip:1001@172.16.119.1

Определить окончательный ответ на запрос *invite*. Ответ будет получен в строке 779:
779 20.247240360 172.16.119.2 172.16.117.31 SIP 392 Status: 480 Temporarily Not Available |

=Status: 480 Temporarily Not Available

В заголовке ответа CSeq указывается, на какой запрос был отправлен данный ответ.

CSeq: 102 INVITE

Услуга "Перевод вызова" (Explisit Call Transfer, ECT).

Для перевода вызова необходимо в программе Twinkle перейти в меню «Сервисы» и выбрать «Перенаправление вызова» (Рисунок 99). Далее необходимо выбрать абонента из списка контактов, кому будет совершен перевод вызова. (Рисунок 100).

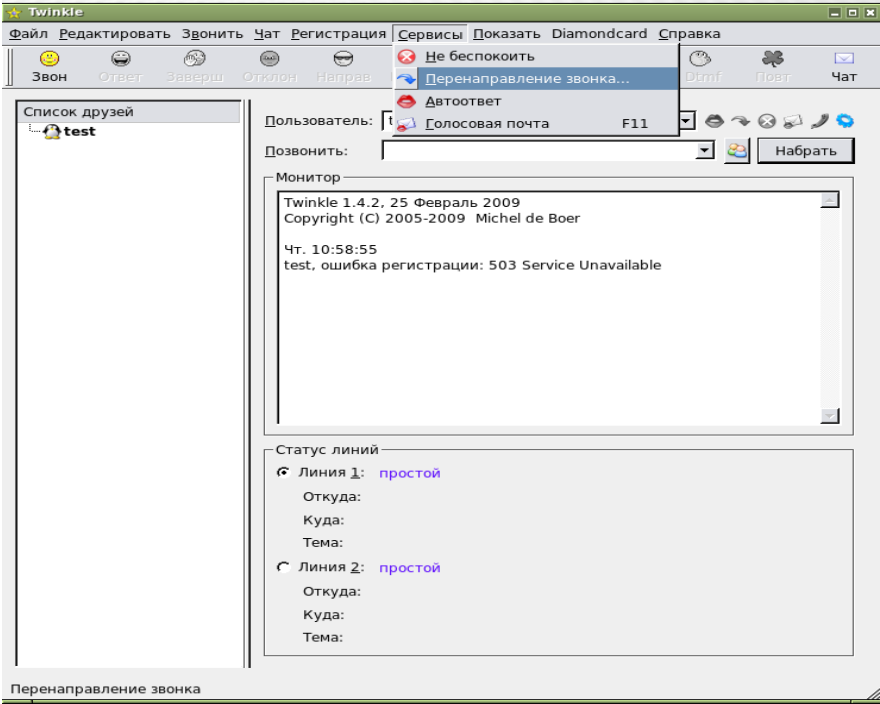


Рисунок 99 Процедура включения режима «Перевод вызова» в программе Twinkle.

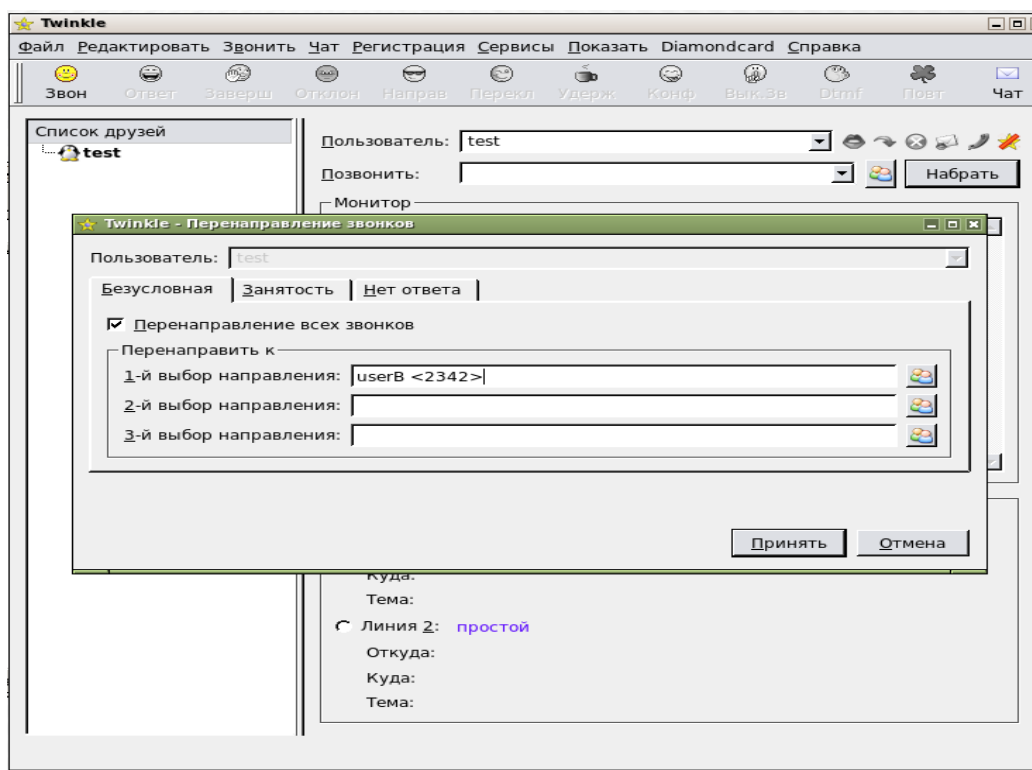


Рисунок 100 Процедура включения режима «Перевод вызова» в программе Twinkle

Посмотрим и проанализируем полученные данные в программной среде *WireShark*. Ниже представлен примерный листинг из данной программы:

```
19 4.596009049 172.16.119.3 172.16.119.4 SIP/SDP 836 Request: INVITE sip:student4@172.16.119.4 |
20 4.597514674 172.16.119.4 172.16.119.3 SIP 320 Status: 100 Trying |
21 4.602309345 172.16.119.4 172.16.119.3 SIP 369 Status: 180 Ringing |
45 7.004386694 172.16.119.4 172.16.119.3 SIP/SDP 707 Status: 200 OK |
48 7.052551767 172.16.119.3 172.16.119.4 SIP 341 Request: ACK sip:student4@172.16.119.4 |
195 8.612860100 172.16.119.3 172.16.119.4 SIP/SDP 858 Request: INVITE sip:student4@172.16.119.4,
in-dialog |
197 8.615149664 172.16.119.4 172.16.119.3 SIP/SDP 719 Status: 200 OK |
201 8.644279888 172.16.119.3 172.16.119.4 SIP 341 Request: ACK sip:student4@172.16.119.4 |
283 30.266139954 172.16.119.3 172.16.119.9 SIP/SDP 899 Request: INVITE sip:student9@172.16.119.9 |
284 30.269476568 172.16.119.9 172.16.119.3 SIP 319 Status: 100 Trying |
285 30.269889221 172.16.119.9 172.16.119.3 SIP 368 Status: 180 Ringing |
327 40.256720253 172.16.119.9 172.16.119.3 SIP/SDP 705 Status: 200 OK |
331 40.292204663 172.16.119.3 172.16.119.9 SIP 340 Request: ACK sip:student9@172.16.119.9 |
574 43.053657052 172.16.119.3 172.16.119.4 SIP 533 Request: REFER sip:student4@172.16.119.4, in-
dialog |
575 43.055180622 172.16.119.4 172.16.119.3 SIP 369 Status: 202 Accepted |
576 43.055731470 172.16.119.4 172.16.119.3 SIP/sipfrag 499 Request: NOTIFY sip:student3@172.16.119.3 |
, with Sipfrag(SIP/2.0 100 Trying...)
578 43.064673702 172.16.119.3 172.16.119.4 SIP 326 Status: 200 OK |
797 46.166338759 172.16.119.9 172.16.119.3 SIP 342 Request: BYE sip:student3@172.16.119.3 |
798 46.167180315 172.16.119.3 172.16.119.9 SIP 324 Status: 200 OK |
799 46.167196484 172.16.119.4 172.16.119.3 SIP/sipfrag 498 Request: NOTIFY sip:student3@172.16.119.3 |
, with Sipfrag(SIP/2.0 100 Trying...)
805 46.205288940 172.16.119.3 172.16.119.4 SIP 326 Status: 200 OK |
806 46.206603273 172.16.119.4 172.16.119.3 SIP/sipfrag 499 Request: NOTIFY sip:student3@172.16.119.3 |
, with Sipfrag(SIP/2.0 180 Ringing...)
807 46.211807563 172.16.119.3 172.16.119.4 SIP 326 Status: 200 OK |
808 46.302580650 172.16.119.4 172.16.119.3 SIP/sipfrag 505 Request: NOTIFY sip:student3@172.16.119.3 |
, with Sipfrag(SIP/2.0 200 OK...)
809 46.302920971 172.16.119.4 172.16.119.3 SIP 341 Request: BYE sip:student3@172.16.119.3 |
810 46.312210545 172.16.119.3 172.16.119.4 SIP 326 Status: 200 OK |
811 46.315745661 172.16.119.3 172.16.119.4 SIP 341 Request: BYE sip:student4@172.16.119.4 |
812 46.316536312 172.16.119.4 172.16.119.3 SIP 323 Status: 200 OK |
813 46.319405141 172.16.119.3 172.16.119.4 SIP 323 Status: 200 OK |
```

Приступим к анализу полученной сигнальной информации:

- определить элементы сети IMS, участвующие в процессе реализации услуги;

Три IMS терминала, P-CSCF, S-CSCF

Определим элементы сети IMS, участвующие в процессе реализации услуги;

Три IMS терминала (Абонент А / Студент 3, Абонент В / Студент 4, Абонент С / Студент 9), P-CSCF, S-CSCF

- определить запрос, осуществляющий перевод вызова с терминала РМ1;

запрос REFER

Чтобы определить запрос, осуществляющий перевод вызова, необходимо найти запрос REFER, который находится под номером 574 в листинге.

574 43.053657052 172.16.119.3 172.16.119.4 SIP 533 Request: **REFER** sip:student4@172.16.119.4, in-dialog |

- определить публичный идентификатор пользователя, на который необходимо осуществить перевод вызова;

заголовок Refer-To

Message Header

Via: SIP/2.0/UDP 172.16.119.3;rport;branch=z9hG4bKvwrylzuz

Max-Forwards: 70

To: <sip:student4@172.16.119.4>;tag=mfqgk

From: <sip:student3@172.16.119.3>;tag=kdfwm

Call-ID: zmlgzsgbcxeaewl@rm-03

CSeq: 74 REFER

Contact: <sip:student3@172.16.119.3>

Refer-To: <sip:student9@172.16.119.9?Replaces=wpokkiovkhabpit%40rm-03%3bto-tag%3disdhi%3bfrom-tag%3dojdr>

Referred-By: <sip:student3@172.16.119.3>

User-Agent: Twinkle/1.4.2

Content-Length: 0

- составить диаграмму обмена сообщениями SIP между всеми участниками соединения при реализации услуги.

Сценарий обмена сообщениями для конкретной ситуации можно получить с помощью программы Wireshark. Для этого необходимо открыть файл сигнальной информации, полученный в результате выполнения задания, и в меню Statistics выбрать раздел VoIP calls -> Graph.

Лабораторная работа №5 «Неудачные попытки установления мультимедийных сессий»

Регистрация и совершение вызова

Проходим процедуру регистрации в сети IMS и подтвердить аккаунт в программе IMS-клиент Monster (*Рисунок 101, Рисунок 102*). Необходимо заполнить данные пользователя (имя и секретный ключ), а также изменить IMSU, после чего уже приступить к подтверждению профиля в программе IMS-клиент Monster (*Рисунок 103*).

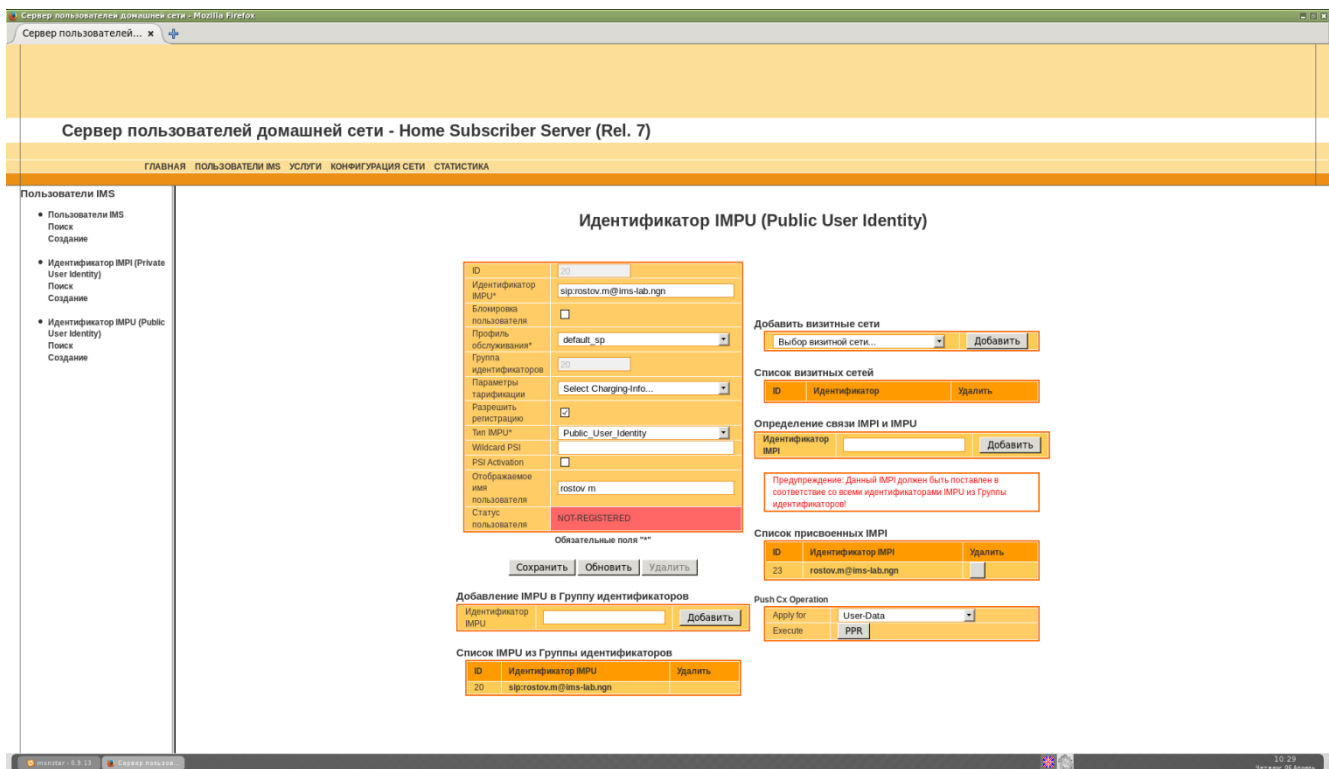


Рисунок 101 – Процедура регистрации пользователя в сети IMS

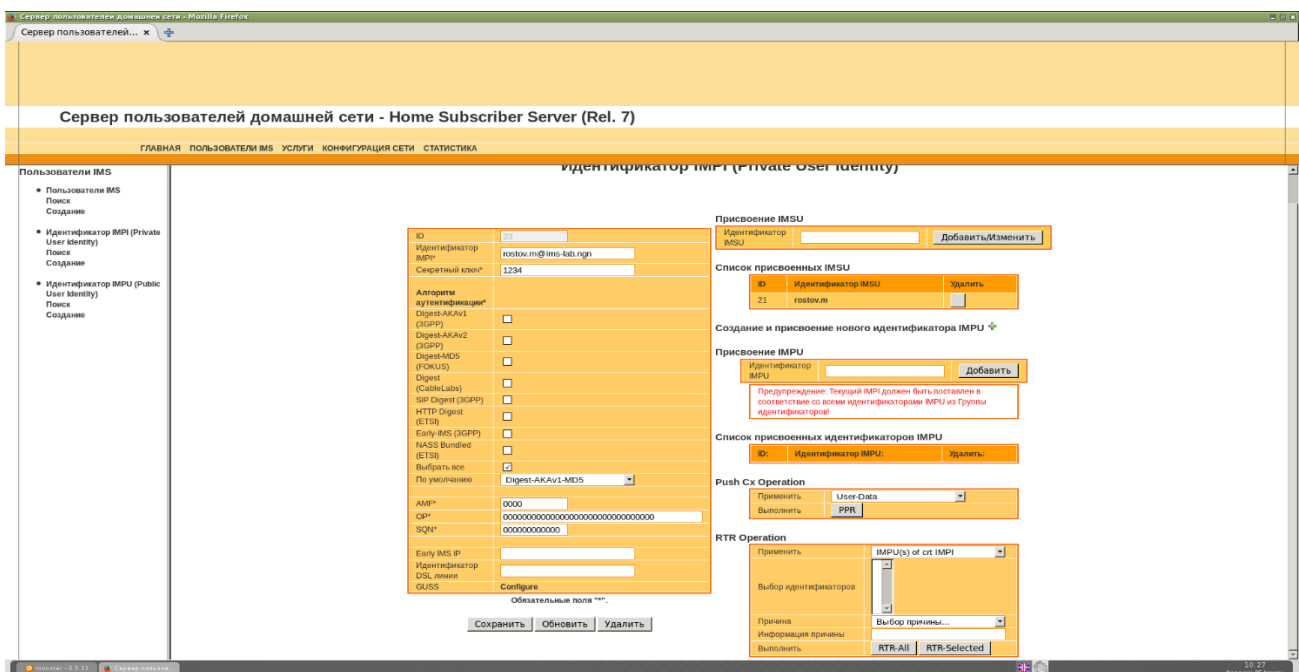


Рисунок 102 – Процедура регистрации пользователя в сети IMS



Рисунок 103 – Подтверждение аккаунта в программе Monster IMS и конфигурация

Далее требуется установить мультимедийную сессии между зарегистрированными пользователями *IMS*, находящимися в домашних сетях.

Запускаем *Wireshark*.

Совершаем звонок в программе *IMS Monster*. Один из пользователей совершает отбой до ответа другого пользователя нажатием кнопки «Cancel / Отмена» (Рисунок 104).

Открываем *Wireshark* и осуществляем фильтрацию по протоколу SIP.

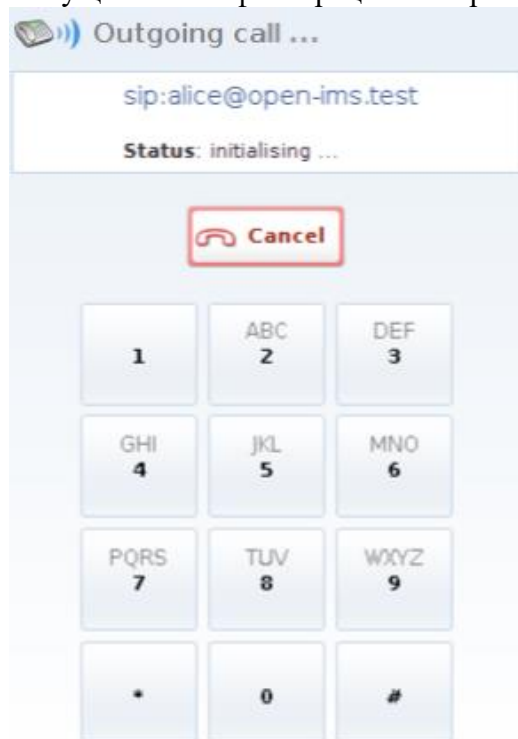


Рисунок 104 – Отбой вызова в IMS Monster

Пользователь *User A* инициирует вызов к пользователю *User B*. Терминальное оборудование пользователя *User A* отправляет сообщение *INVITE* протокола *SIP* для запроса установления мультимедийной сессии с пользователем *User B*, содержащее описание сессии в формате *SDP* для передачи данных от *User B* к *User A*. *P-CSCFA* принимает запрос *INVITE*, заменяет в запросе *INVITE* заголовок *P-Preferred-Identity* на заголовок *P-Asserted-Identity*, содержащий зарегистрированный идентификатор *PuUI* вызывающего пользователя, добавляет в заголовок *Route* свой адрес и отправляет запрос к функциональному объекту *S-CSCFA*. К оборудованию вызываемого пользователя *P-CSCFA* отправляет ответ с кодом *100 (Trying)*. Этот ответ информирует терминал о том, что запрос *INVITE* был получен, и прокси-сервер выполняет маршрутизацию запроса к месту назначения. *S-CSCFA* на основании идентификатора пользователя *User B*, содержащегося в запросе *INVITE*, определяет входную точку в домашнюю сеть вызываемого пользователя *I-CSCFB*. После чего отправляет запрос *INVITE* к *I-CSCFB*, а к *P-CSCFA* ответ *100 (Trying)*. Ниже представлен примерный листинг из программы *WireShark*:

Отбой вызывающего пользователя в предответном состоянии

Примерный листинг пакетов, отфильтрованных по протоколу *SIP*:

15	3.372971496	172.16.119.10	172.16.117.22	SIP	635	Request: REGISTER sip:ngn.lab (1 binding)
16	3.387887496	172.16.117.22	172.16.119.10	SIP	984	Status: 401 Unauthorized - Challenging the UE
17	3.469545664	172.16.119.10	172.16.117.22	SIP	781	Request: REGISTER sip:ngn.lab (1 binding)
18	3.490371454	172.16.117.22	172.16.119.10	SIP	1022	Status: 200 OK - SAR succesful and registrar saved
19	4.410520763	172.16.119.10	172.16.117.22	SIP/XML	861	Request: PUBLISH sip:ivanov.a@ngn.lab
20	4.412476556	172.16.117.22	172.16.119.10	SIP	459	Status: 200 OK
33	20.233379865	172.16.119.10	172.16.117.22	SIP/SDP	772	Request: INVITE sip:rostov.m@ngn.lab
34	20.234219249	172.16.117.22	172.16.119.10	SIP	600	Status: 100 trying -- your call is important to us
35	20.313726698	172.16.117.22	172.16.119.10	SIP	587	Status: 180 Ringing
40	27.082674611	172.16.119.10	172.16.117.22	SIP	432	Request: CANCEL sip:rostov.m@ngn.lab
41	27.083448150	172.16.117.22	172.16.119.10	SIP	613	Status: 200 canceling
42	27.099953275	172.16.117.22	172.16.119.10	SIP	444	Status: 487 Request terminated
43	27.103541247	172.16.119.10	172.16.117.22	SIP	392	Request: ACK sip:rostov.m@ngn.lab

- определить запрос, который используется при отбое вызывающего пользователя в предответном состоянии и ответ на него;

Запрос Cancel и ответ на него 200 OK

Необходимо найти строку 40 и 41, выделенную пунктиром;

40	27.082674611	172.16.119.10	172.16.117.22	SIP	432	Request: CANCEL sip:rostov.m@ngn.lab
41	27.083448150	172.16.117.22	172.16.119.10	SIP	613	Status: 200 canceling

Запрос: CANCEL и ответ на него 200 OK

- определить окончательный ответ на запрос *INVITE*.

Ответ 487 Request Terminated

В строке 42 находим ответ

42	27.099953275	172.16.117.22	172.16.119.10	SIP	444	Status: 487 Request terminated
----	--------------	---------------	---------------	-----	-----	--------------------------------

Вызов пользователя, отсутствующего в сети

Необходимо осуществить вызов от пользователя *PM 1* к пользователю, учетная запись которого прописана в базе данных пользователей *HSS*, но не активирована ни на одном из терминалов. Далее заходим в *WireShark* и анализируем полученные данные (в примере рассмотрен возможный вариант).

Примерный листинг программы *WireShark*:

23	37.120851348	172.16.119.10	172.16.117.22	SIP/SDP	772	Request: INVITE sip:rostov.q@ngn.lab
24	37.121869214	172.16.117.22	172.16.119.10	SIP	600	Status: 100 trying -- your call is important to us
26	37.127096297	172.16.117.22	172.16.119.10	SIP	646	Status: 604 Does not exist anywhere - HSS User Unknown
27	37.129382952	172.16.119.10	172.16.117.22	SIP	425	Request: ACK sip:rostov.q@ngn.lab
32	42.717958634	172.16.119.10	172.16.117.22	SIP/SDP	772	Request: INVITE sip:rostov.m@ngn.lab
33	42.718656099	172.16.117.22	172.16.119.10	SIP	600	Status: 100 trying -- your call is important to us
34	42.738255492	172.16.117.22	172.16.119.10	SIP	587	Status: 180 Ringing
41	51.142773236	172.16.119.10	172.16.117.22	SIP	432	Request: CANCEL sip:rostov.m@ngn.lab
42	51.143430619	172.16.117.22	172.16.119.10	SIP	613	Status: 200 canceling
43	51.158901185	172.16.117.22	172.16.119.10	SIP	444	Status: 404 Not found
44	51.161308888	172.16.119.10	172.16.117.22	SIP	392	Request: ACK sip:rostov.m@ngn.lab

По сигнальной информации, полученной с помощью программы Wireshark:

- определить элементы сети IMS, участвующие в процессе установления мультимедийной сессии;

IMS терминал, P-CSCF, S-CSCF, I-CSCF, HSS

- определить сообщения SIP (запросы и ответы) и сообщения DIAMETER, отправленные для установления сессии, по сигнальной информации, полученной с помощью программы Wireshark;

необходимо найти строку 23

Для установления соединения отправляется запрос INVITE протокола SIP

23 37.120851348 172.16.119.10 172.16.117.22 SIP/SDP 772 Request: INVITE sip:rostov.q@ngn.lab |

- определить в каких сообщениях SIP и Diameter передается информация о невозможности установить сессию.

В ответе 404 Not found протокола SIP и в сообщении Location-InfoAnswer.

Необходимо найти строку 43:

43 51.158901185 172.16.117.22 172.16.119.10 SIP 444 Status: 404 Not found |

- Составить диаграмму обмена сообщениями между всеми участниками сессии.

Сценарий обмена сообщениями для конкретной ситуации можно получить с помощью программы Wireshark. Для этого необходимо открыть файл сигнальной информации, полученный в результате выполнения задания, и в меню Statistics выбрать раздел VoIP calls -> Graph.

Для того, чтобы составить диаграмму обмена сообщениями между всеми участниками соединения, необходимо в Wireshark перейти в Telephony > VoIP Calls и выбрать участников звонка, а затем нажать «Graph». Результат представлен на Рисунок 105 .

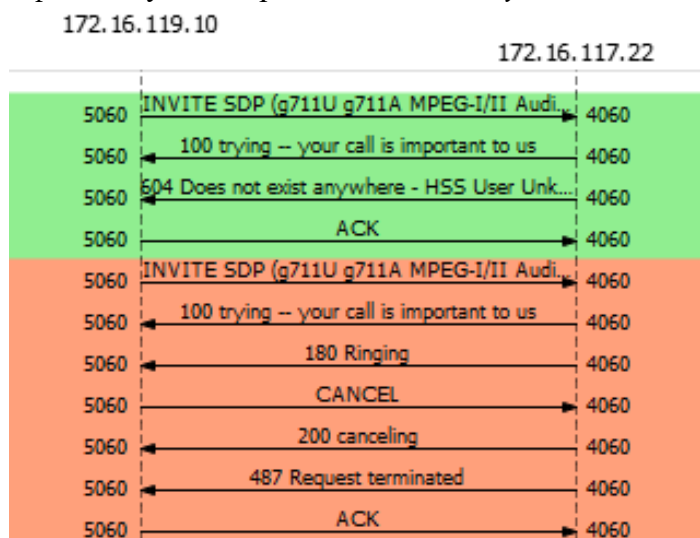


Рисунок 105 – Диаграмма обмена сообщениями

Вызов несуществующего пользователя

Необходимо осуществить вызов от пользователя РМ 1 к пользователю, учетная запись которого не прописана в базе данных пользователей HSS. Далее заходим в *WireShark* и анализируем полученные данные (в примере рассмотрен возможный вариант).

Примерный листинг программы *WireShark*:

```
23 37.120851348 172.16.119.10 172.16.117.22 SIP/SDP 772 Request: INVITE sip:rostov.q@ngn.lab |
24 37.121869214 172.16.117.22 172.16.119.10 SIP 600 Status: 100 trying -- your call is important to us |
26 37.127096297 172.16.117.22 172.16.119.10 SIP 646 Status: 604 Does not exist anywhere - HSS User
Unknown |
27 37.129382952 172.16.119.10 172.16.117.22 SIP 425 Request: ACK sip:rostov.q@ngn.lab |
32 42.717958634 172.16.119.10 172.16.117.22 SIP/SDP 772 Request: INVITE sip:rostov.m@ngn.lab |
33 42.718656099 172.16.117.22 172.16.119.10 SIP 600 Status: 100 trying -- your call is important to us |
34 42.738255492 172.16.117.22 172.16.119.10 SIP 587 Status: 180 Ringing |
41 51.142773236 172.16.119.10 172.16.117.22 SIP 432 Request: CANCEL sip:rostov.m@ngn.lab |
42 51.143430619 172.16.117.22 172.16.119.10 SIP 613 Status: 200 canceling |
43 51.158901185 172.16.117.22 172.16.119.10 SIP 444 Status: 487 Request terminated |
44 51.161308888 172.16.119.10 172.16.117.22 SIP 392 Request: ACK sip:rostov.m@ngn.lab |
```

По сигнальной информации, полученной с помощью программы *Wireshark*:

- определить элементы сети IMS, участвующие в процессе установления мультимедийной сессии;

IMS терминал, P-CSCF, S-CSCF, I-CSCF, HSS

- определить сообщения SIP (запросы и ответы) и сообщения DIAMETER, отправленные для установления сессии;

Для установления соединения отправляется запрос INVITE протокола SIP

Необходимо найти строку 23

```
23 37.120851348 172.16.119.10 172.16.117.22 SIP/SDP 772 Request: INVITE sip:rostov.q@ngn.lab |
```

- определить, в каких сообщениях SIP и Diameter передается информация о невозможности установить сессию.

В ответе класса 6XX протокола SIP и в сообщении Location-InfoAnswer.

Необходимо найти строку 26

```
26 37.127096297 172.16.117.22 172.16.119.10 SIP 646 Status: 604 Does not exist
anywhere - HSS User Unknown |
```

- Составить диаграмму обмена сообщениями между всеми участниками соединения.

Сценарий обмена сообщениями для конкретной ситуации можно получить с помощью программы Wireshark. Для этого необходимо открыть файл сигнальной информации, полученный в результате выполнения задания, и в меню Statistics выбрать раздел VoIP calls -> Graph.

Приложение 1. Создание пользователя, зарегистрированного на сервере Asterisk, в программном телефоне Twinkle.

Выбор настройки терминала с помощью "Мастера" (рис. 1).

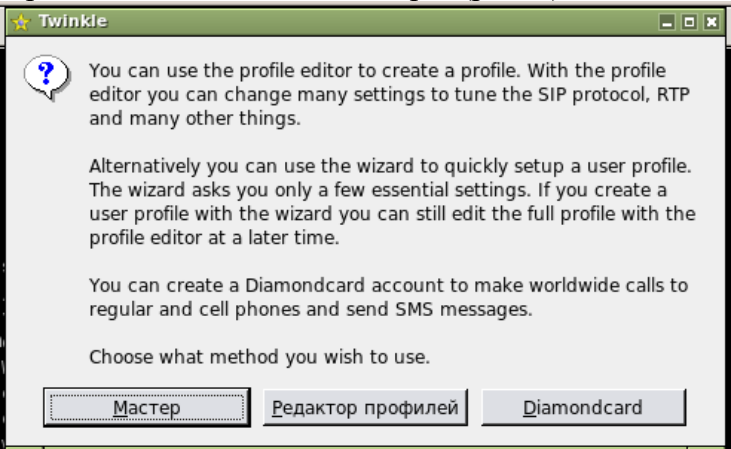


Рис. 1. Окно настройки профилей Twinkle

Ввести имя профиля соответствующее нумерации в сети и в соответствии с заданием (рис. 2).

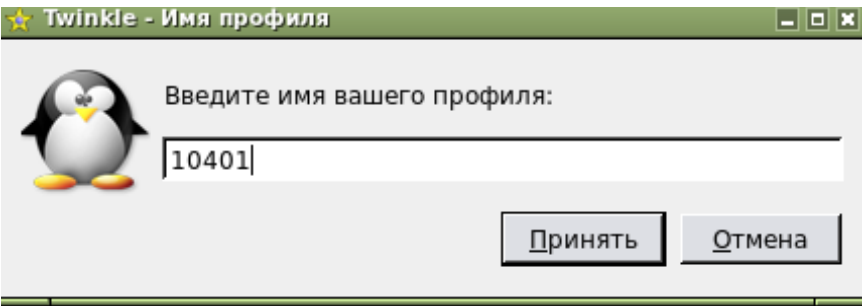


Рис. 2. Окно «Profile name» (Имя профиля)

Задать поля "Ваше имя", "Имя пользователя", записать в них соответствующую заданию нумерацию.

Задать поле "Домен", записать в нем "172.16.119.Z" (рис. 3).

В шаблоне вместо символа Z прописывается последнее число адреса РМ на сервере Asterisk.

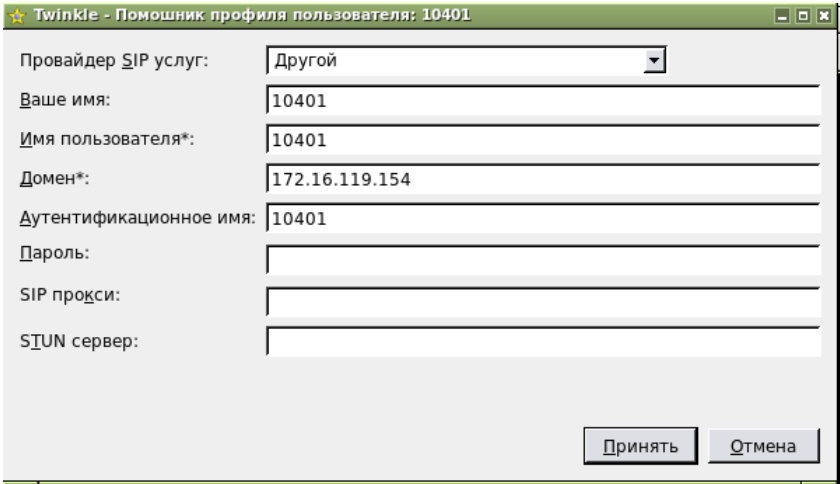


Рис. 3. Окно настройки профиля

Выбрать стандартный профиль пользователя, созданный ранее (рис. 4).

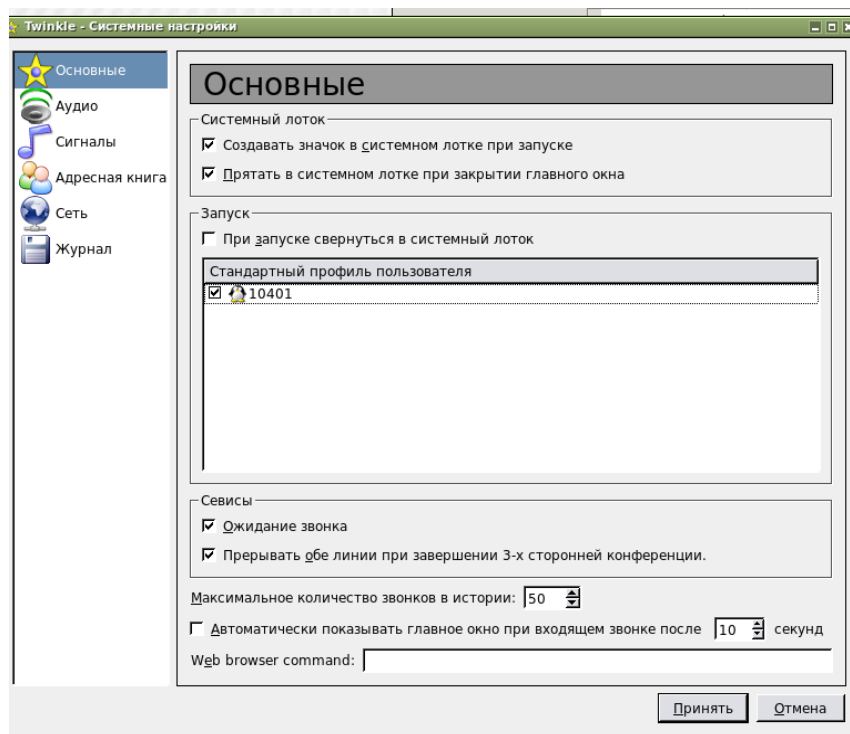


Рис. 4. Окно системных настроек «System settings» (подменю «Основное»)

Выбрать подменю в левой части программного телефона - «Сеть».
Изменить значение поля «SIP port» на «5063» (рис. 5).

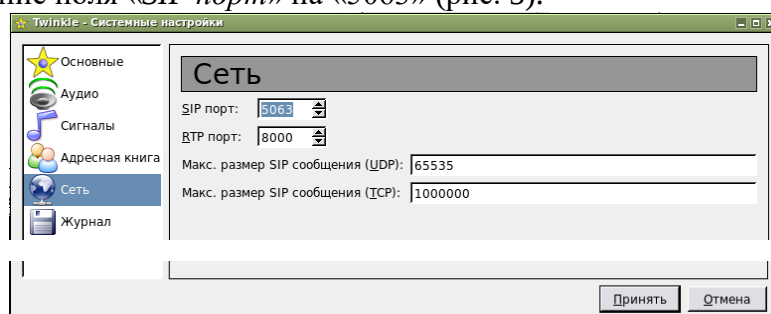


Рис. 5. Окно системных настроек «System settings» (подменю «Сеть»)

Нажать кнопку «Принять». Регистрация завершена (рис. 6).

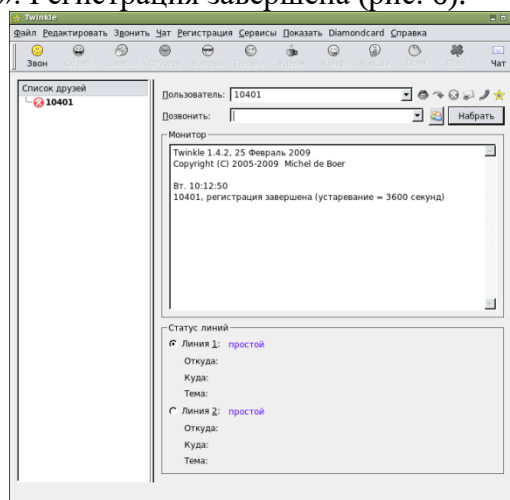


Рис. 6. Окно зарегистрированного пользователя в Twinkle

Приложение 2. Создание пользователя, зарегистрированного на сервере Asterisk, в программном телефоне Linphone.

При первом запуске программного телефона *Linphone* откроется помощник настройки учетной записи SIP. Нажать «Forward» (рис. 1).

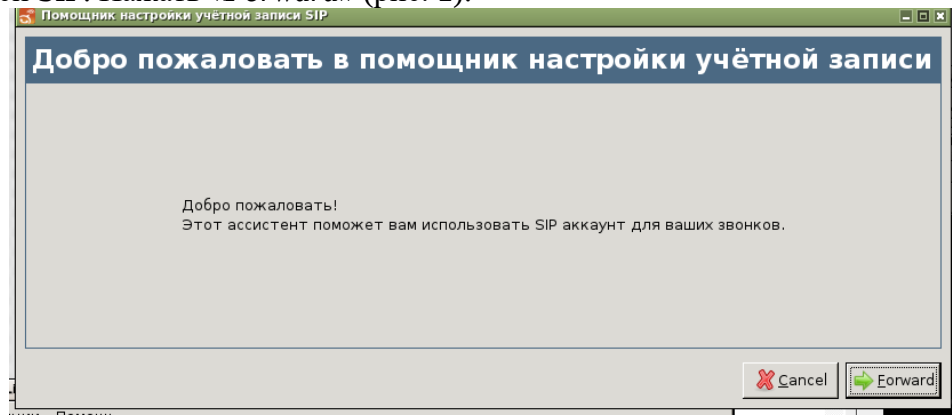


Рис. 1. Помощник настройки учетной записи

Выбрать пункт «Я уже имею учетную запись sip и только хочу использовать её». Нажать «Forward» (рис. 2).



Рис. 2. Помощник настройки учетной записи (меню)

Задать поле "Имя пользователя", записать в нем соответствующую заданию нумерацию (рис. 3).

Задать поле "Домен", записать в нем "172.16.119.Z". Нажать «Apply» (рис. 3).

В шаблоне вместо символа Z прописывается последнее число адреса РМ на сервере Asterisk.

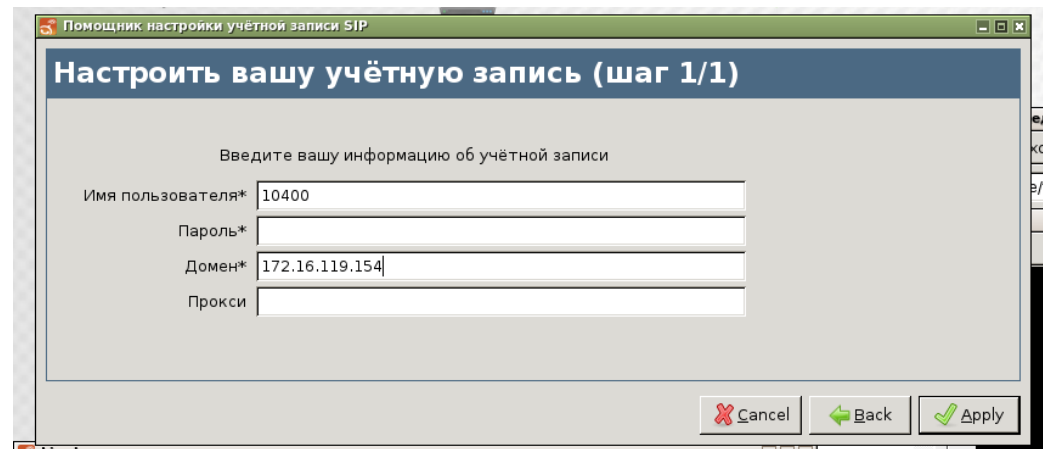


Рис. 3. Настройка учетной записи

Выбрать пункт *Preferences* в меню *Опции* программного телефона *LinPhone* (рис. 4).

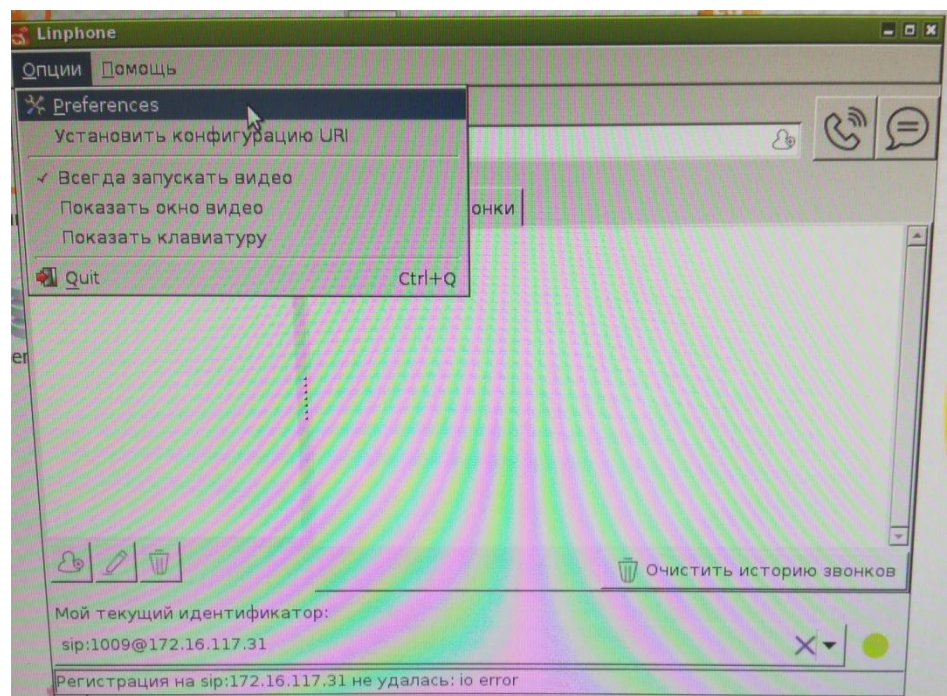


Рис. 4. Главное окно Linphone

Выбор окна настройки сети. В области «Сетевые протоколы и порты» изменить значения полей «порт SIP/UDP» и «порт SIP/TCP» на «5062» (рис. 6).

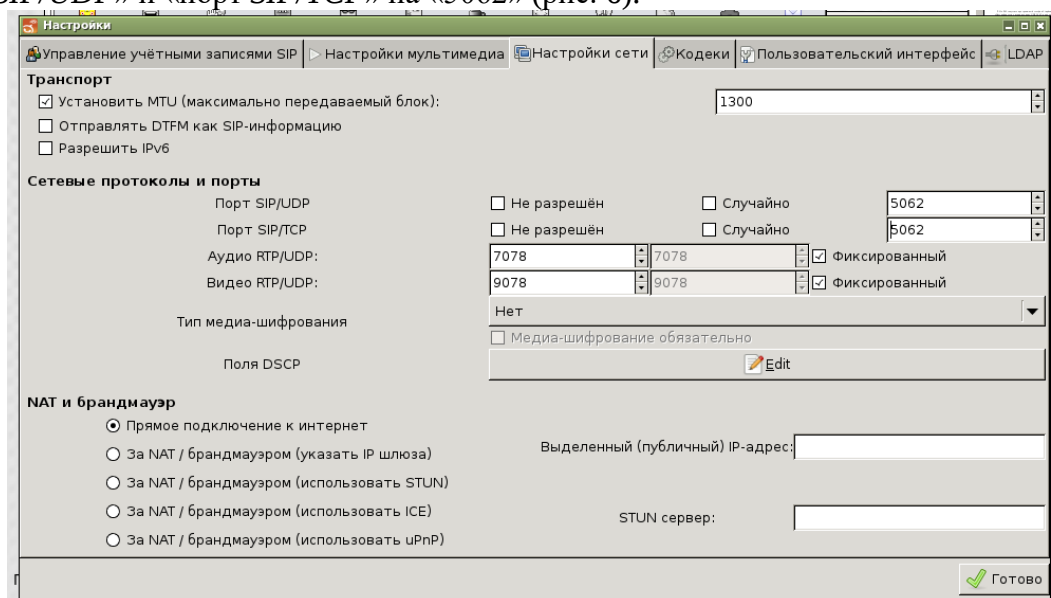


Рис. 5. Окно настройки сети

Выбор окна «Управление учетными записями SIP».

Выбор настройки учетных записей с помощью кнопки "Редактировать" (рис. 6).

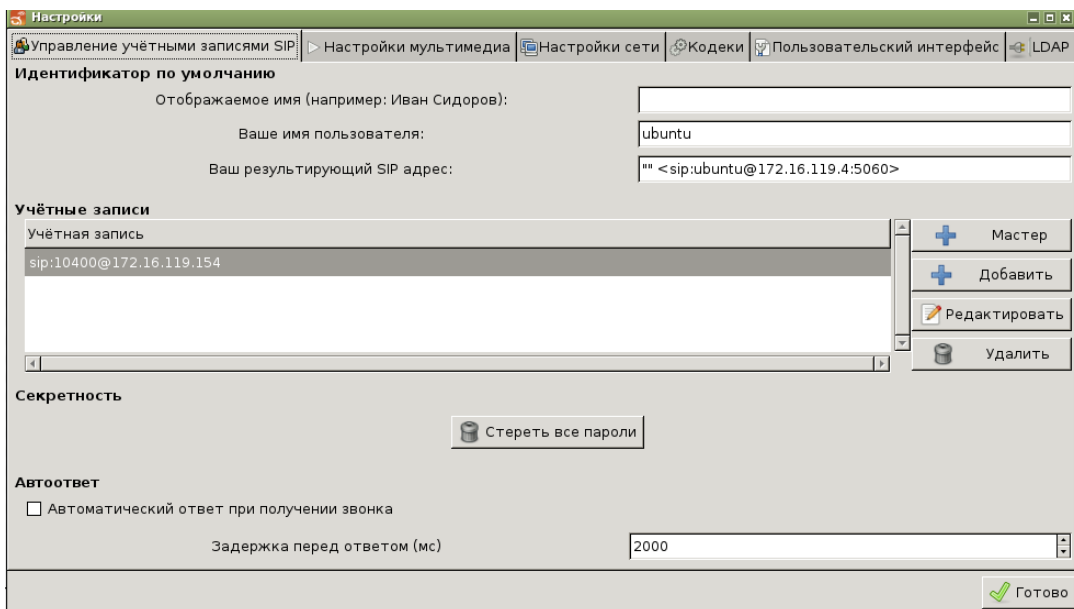


Рис. 6. Окно профилей пользователя

Ввести в поле «Ваш идентификатор SIP» "*sip:{соответствующая нумерация}@172.16.119.Z*".

Задать поле "Адрес SIP прокси", записать в нем "*<sip: :{соответствующая нумерация}@172.16.119.Z;transport=udp>*".

Указать Транспорт "UDP".

Отметить пункты "Регистрация", "Опубликовать статус присутствия" (рис. 7).

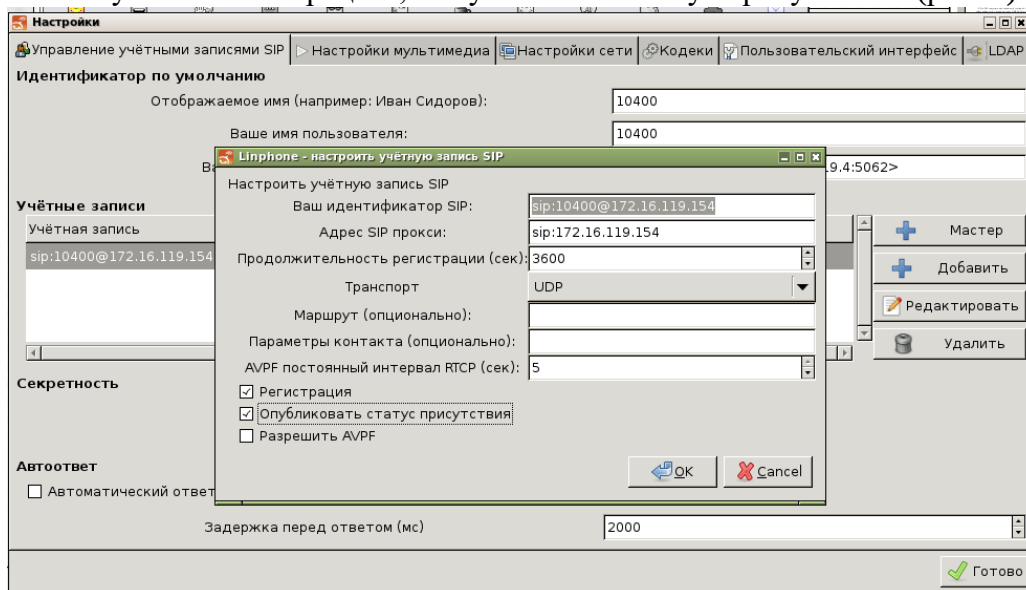


Рис. 7. Окно настройки профиля пользователя

Нажать "Ок".

В области «Идентификатор по умолчанию» задать поля "Отображаемое имя", "Ваше имя пользователя", записать в них соответствующую нумерацию (рис. 8).

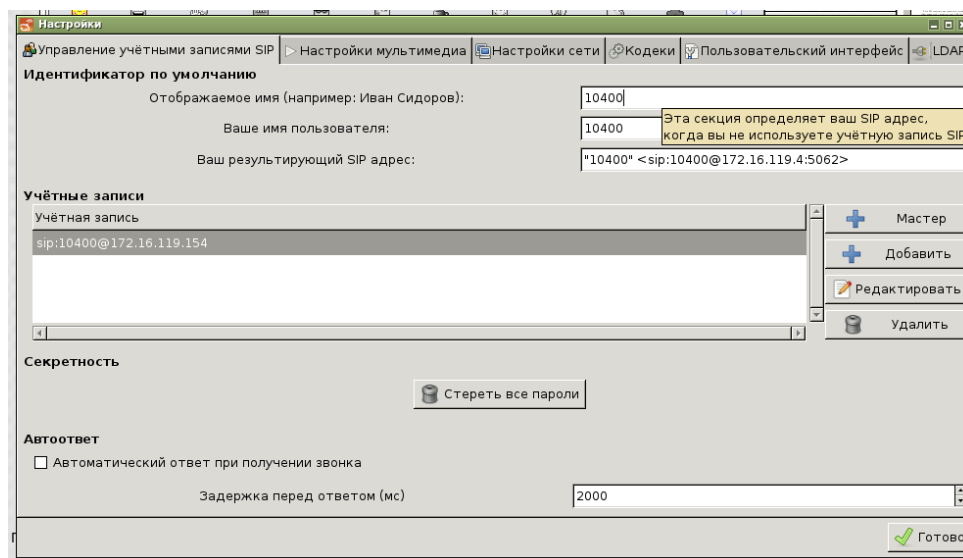


Рис. 8. Окно профилей пользователя

Нажать «Готово». Регистрация завершена (рис. 9).

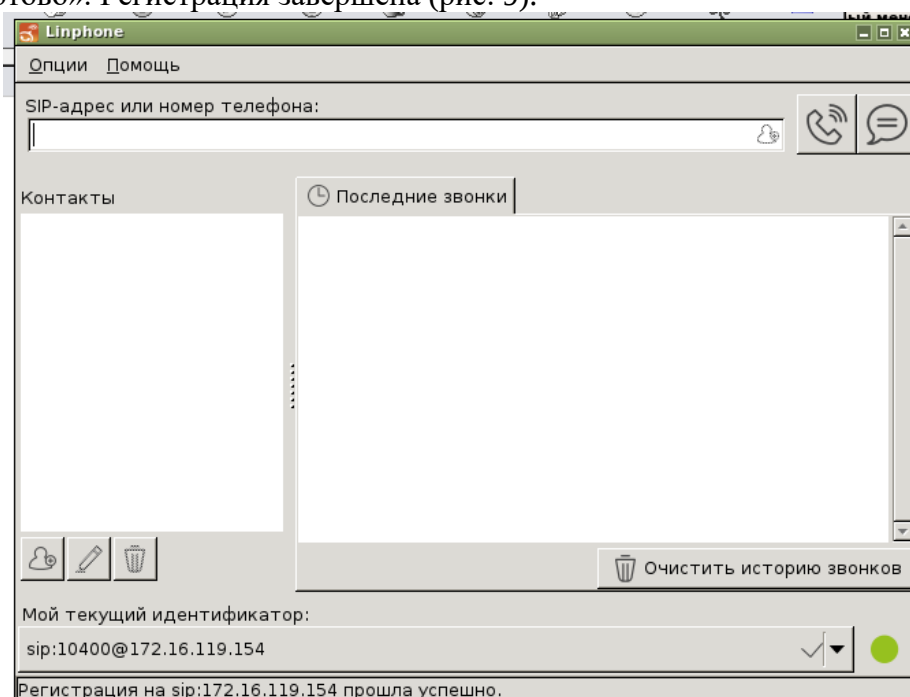


Рис. 9. Окно зарегистрированного пользователя в Linphone

Приложение 3. Работа в терминале.

Работа в терминале производится по следующим шагам:

- для вызова консоли (терминала) кликните дважды на иконку «Управление Asterisk CLI» (рис. 1). При вызове консоли данным методом пользователь получает права администратора и может изменять файлы;
- для работы в данной консоли существуют множество различных команд;
- для перехода в режим просмотра файлов и каталогов необходимо ввести в консоль команду «mc» и нажать клавишу «Enter»;

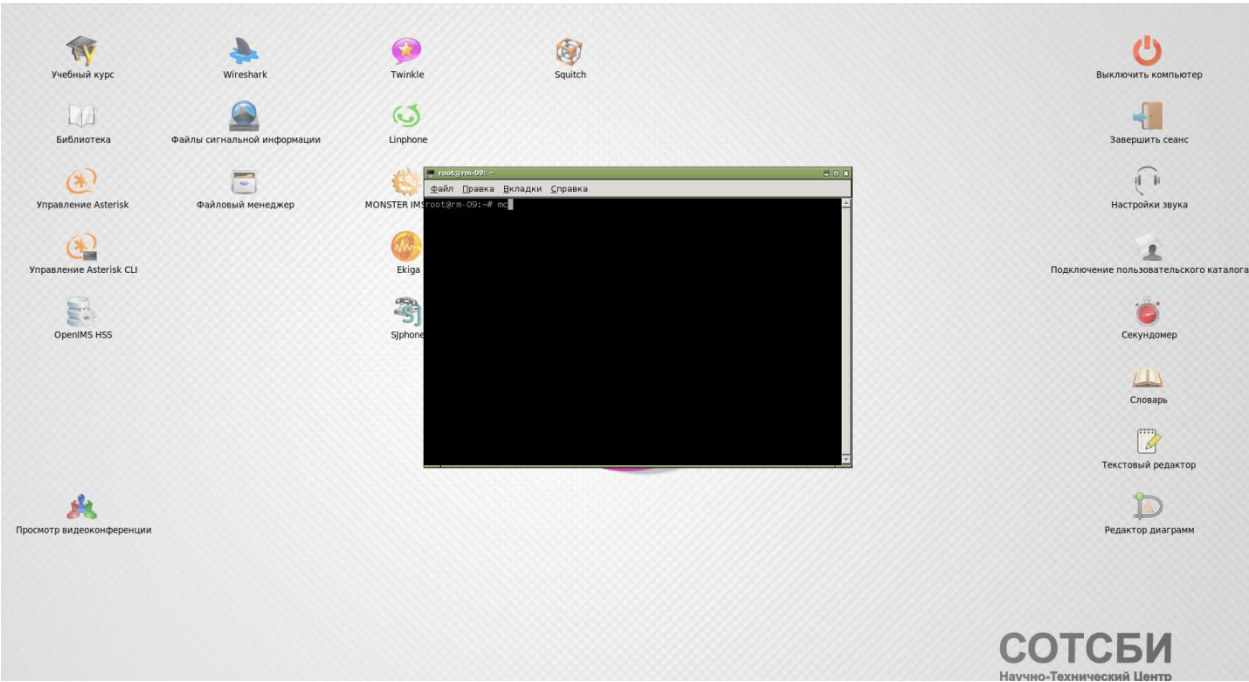


Рис. 1. Консоль с правами администратора

После перехода в режим просмотра каталогов, появляется следующее окно (рис. 2)

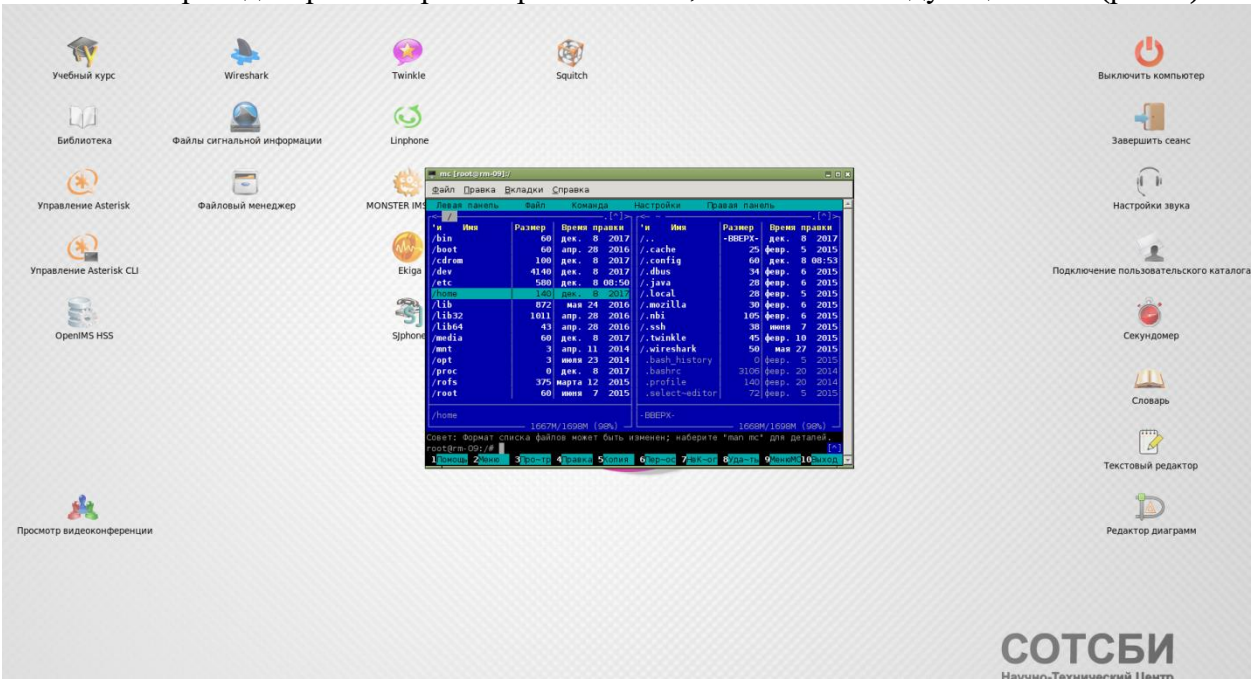


Рис. 2. Консоль, режим просмотра каталогов

- для перехода в каталог необходимо дважды кликнуть на имя нужного каталога;

- для перехода в предыдущий каталог необходимо дважды кликнуть на знак «/..», расположенный выше всех каталогов и файлов (рис. 3);

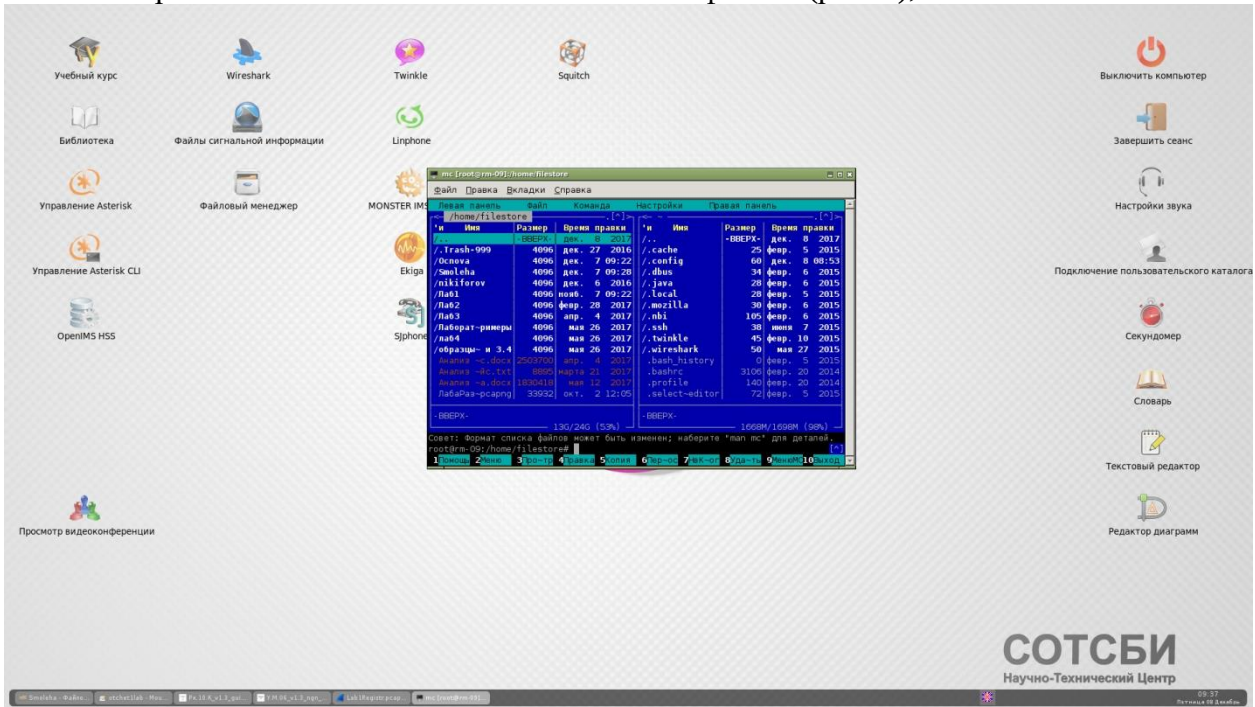


Рис. 3. Консоль, переход в предыдущий каталог

- для просмотра файла необходимо выбрать файл, нажать на него один раз, затем нажать на кнопку «Просмотр» в нижней части консоли. После этого действия откроется выбранный файл в режиме просмотра (рис. 4);

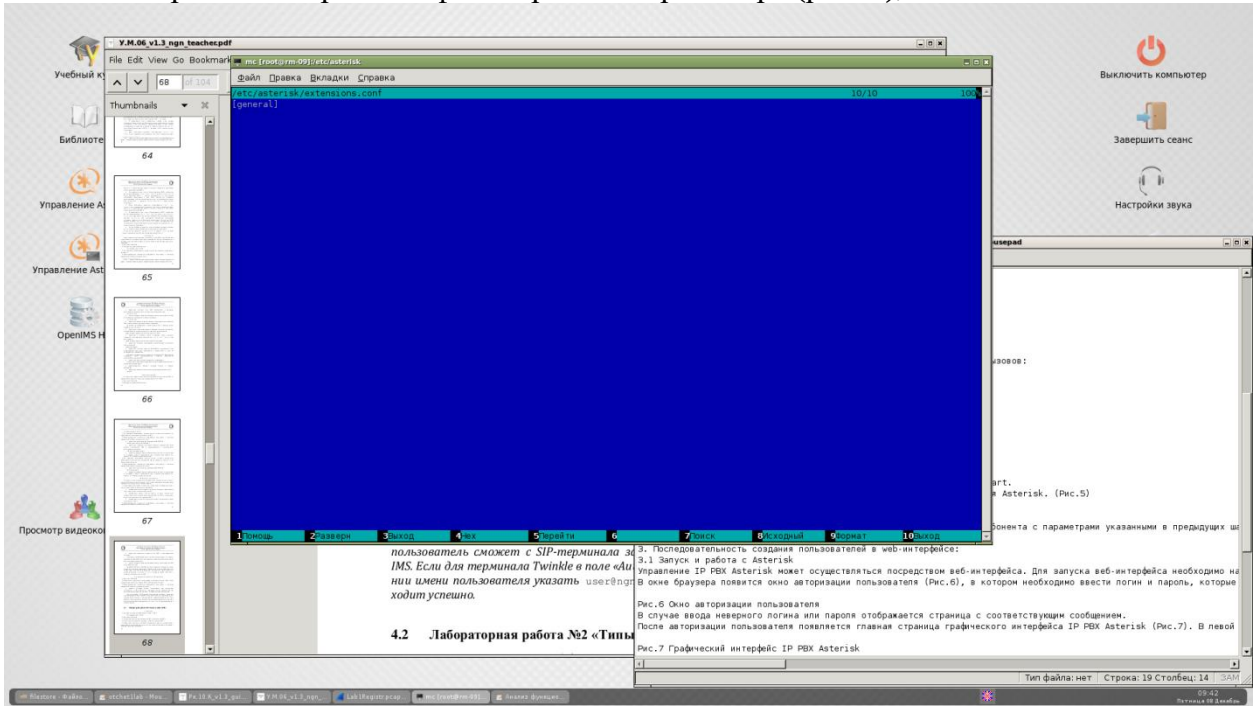


Рис. 4. Консоль, файл в режиме просмотра

- для изменения файла необходимо выбрать файл, нажать на него один раз, затем нажать на кнопку «Правка» в нижней части консоли. После этого действия откроется выбранный файл в режиме изменения (рис. 5). После изменения файла необходимо нажать на кнопку «Сохранить» в нижней части консоли;
- для вставки скопированных данных в файл необходимо нажать правой кнопкой

мышью в области тела файла и выбрать пункт из всплывающего списка – «Вставить»;

Примечание: Сочетание клавиш «Ctrl+x» «Ctrl+c» «Ctrl+v» в режиме изменения файла не работают!

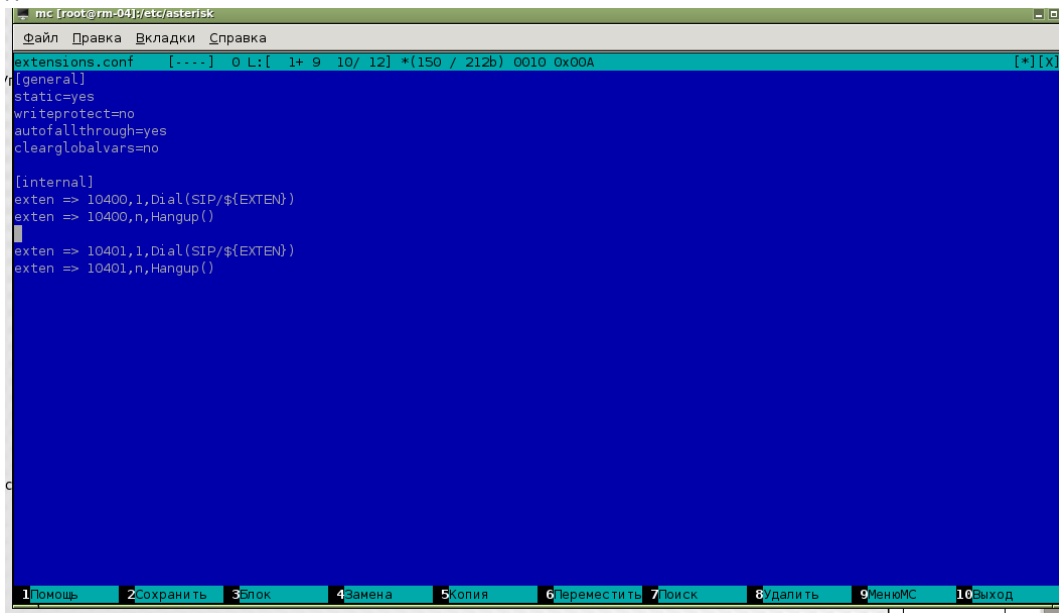


Рис. 5. Консоль, файл в режиме изменения (правки)

- для удаления записей в файле используется клавиша «Backspace», либо выделив необходимый текст в файле нажать на кнопку «Удалить»;
- для выхода из режимов просмотра и изменения файла необходимо нажать на кнопку «Выход» (рис. 4 и рис. 5);
- для выхода из режима просмотра каталогов необходимо нажать на кнопку «Выход» и в появившемся меню нажать на кнопку «Да» (рис. 6). После этого действия появится консоль (рис.1).

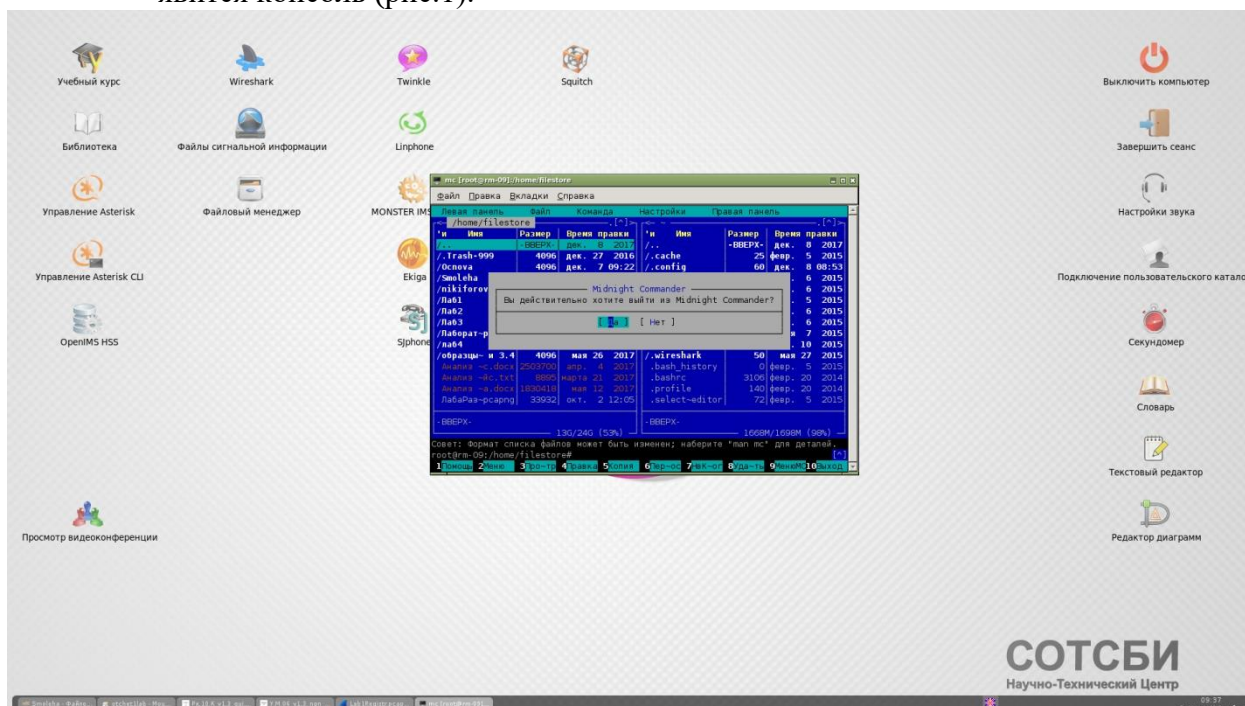


Рис. 6. Консоль, выход из Midnight Commander

Создание и редактирование файлов в терминале.

Примечание: Вместо имени файла можно указывать полный путь к нему. Для создания и редактирования файлов необходимо зайти в консоль с правами администратора (Зайти в консоль

на рабочем столе «Управление Asterisk CLI»).

Для создания файла необходимо ввести команду “touch «имя файла» “ (рис. 7). В случае, если данный файл уже существует в каталоге, то файл перезапишется (станет пустым).

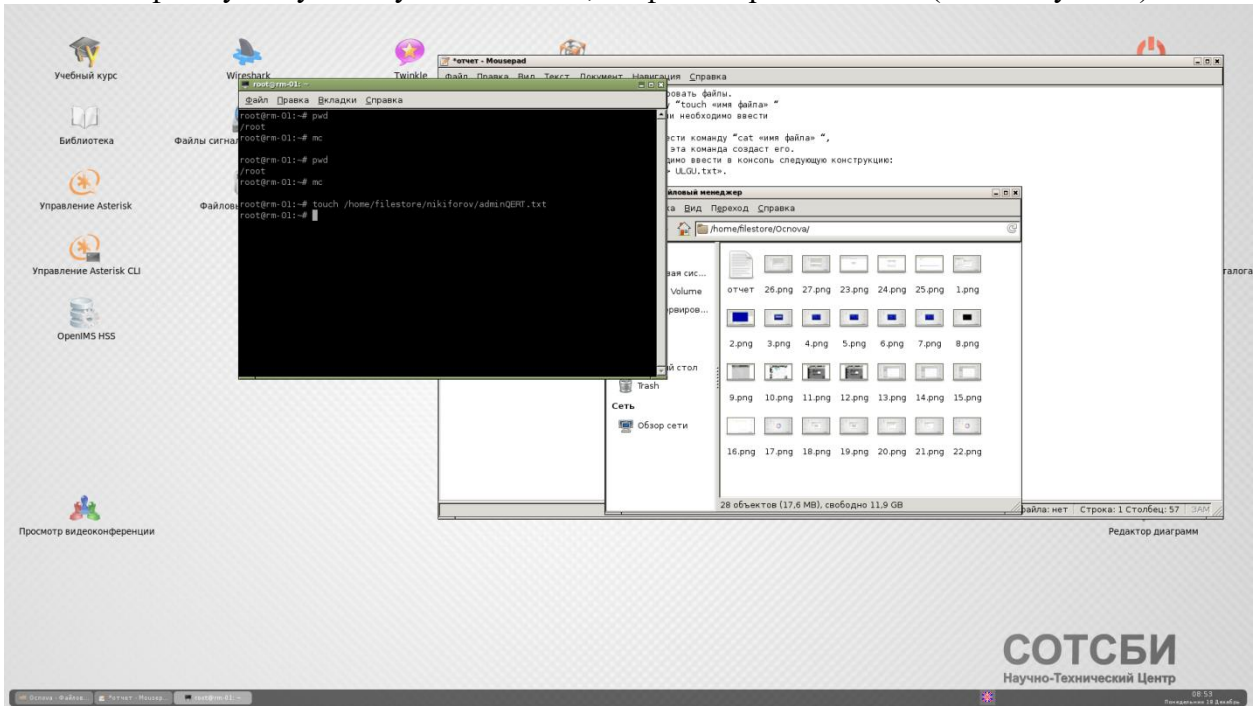


Рис. 7. Команда touch

Для добавления в конец файла новой информации необходимо ввести команду “echo «информация» >> «имя файла»” (рис. 8).

Для просмотра файла в консоли необходимо ввести команду “cat «имя файла» “, если такого файла в данном каталоге нет, то эта команда создаст его (рис. 8).

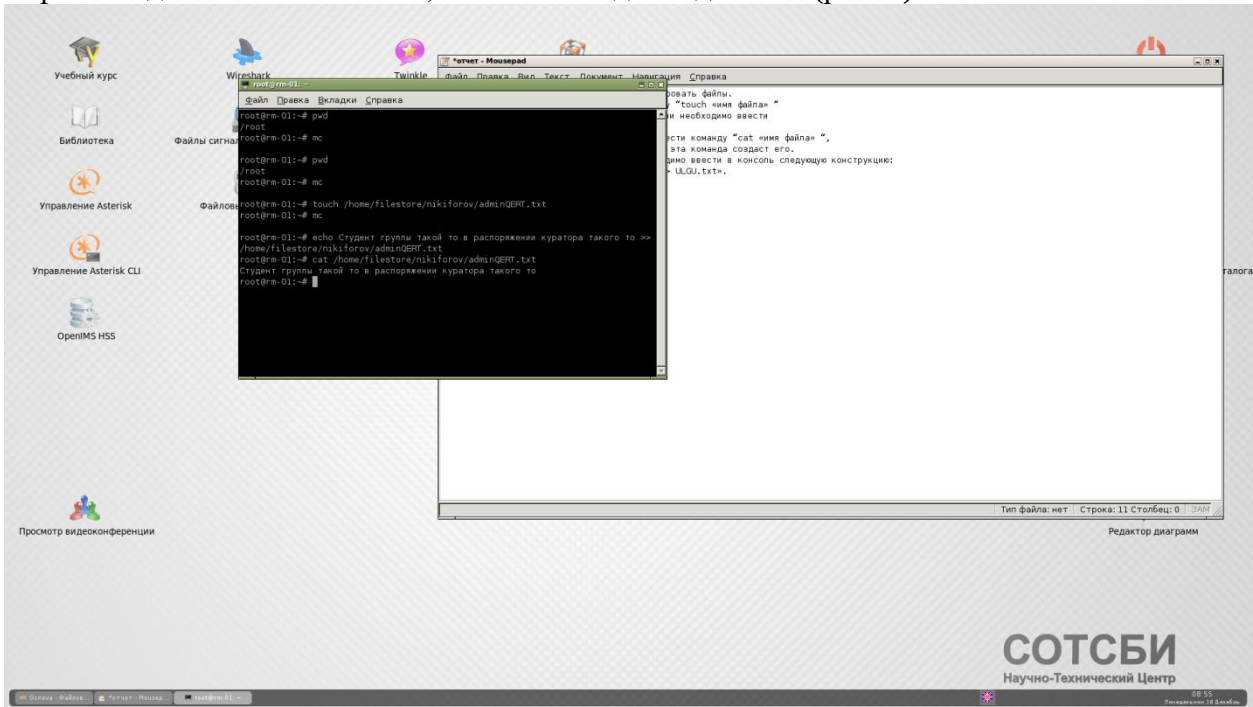


Рис. 8. Команды cat и echo

После проведенных действий в каталоге появиться текстовый файл (рис. 9, рис. 10)

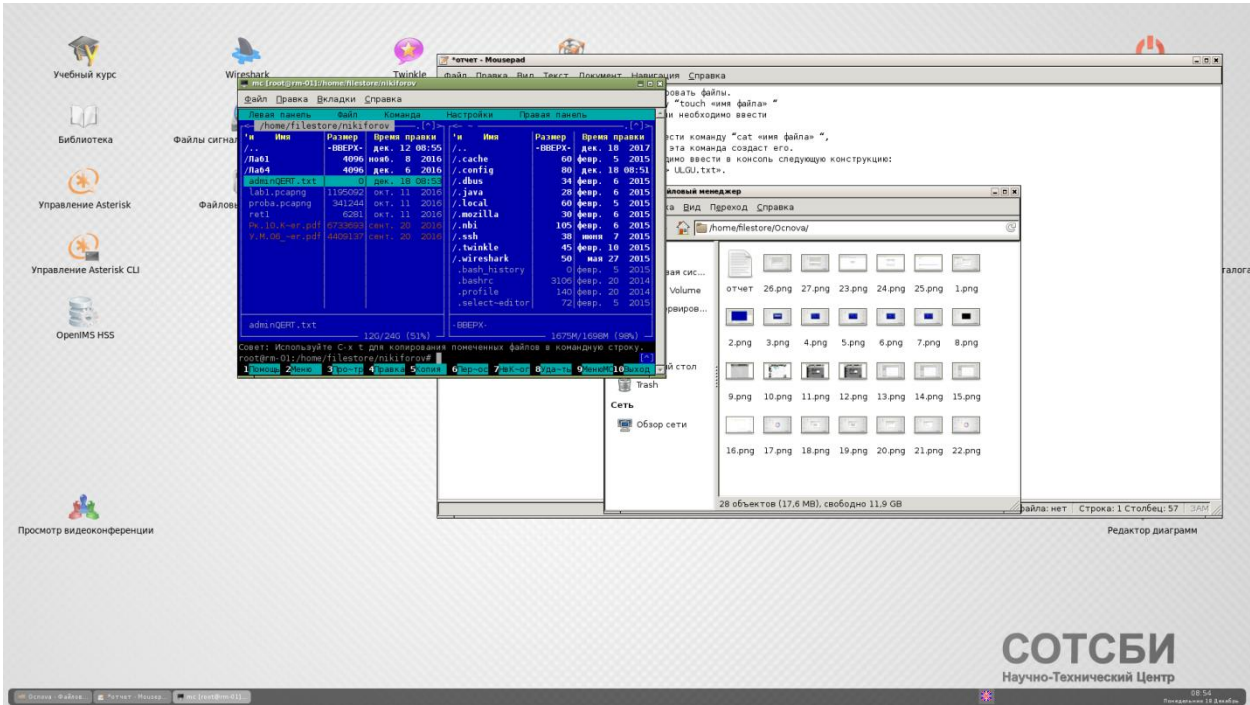


Рис. 9. Созданный файл

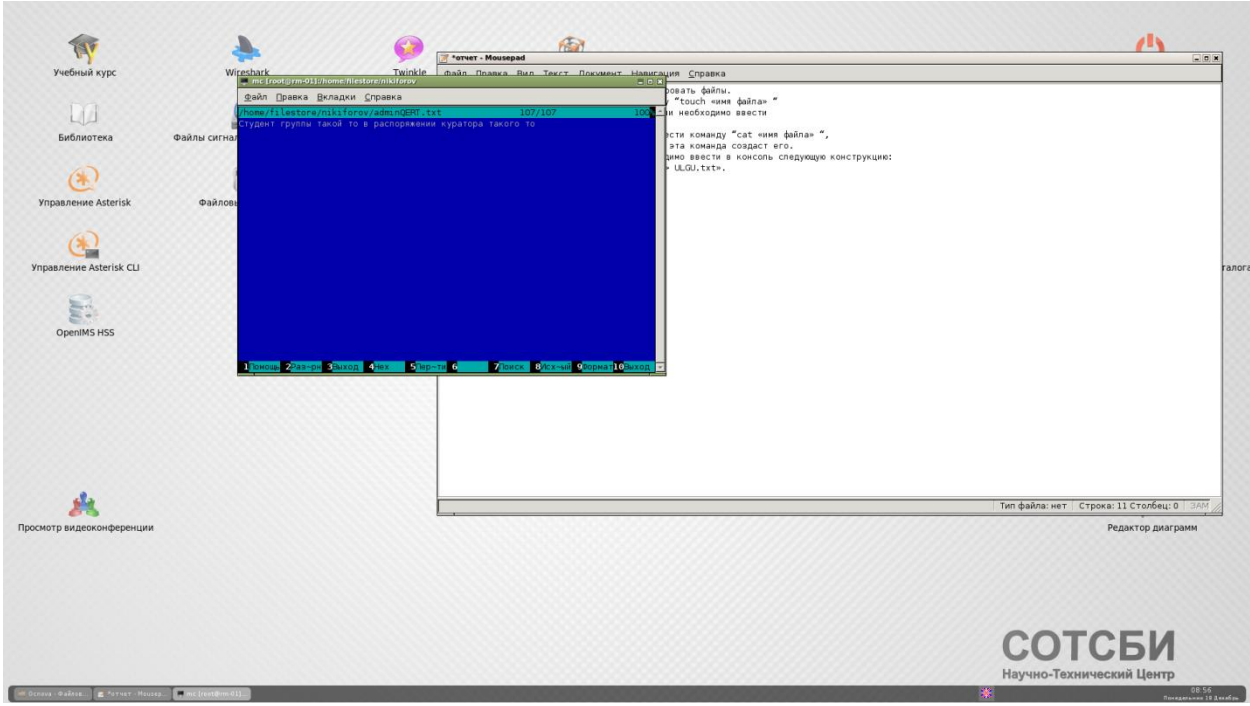


Рис. 10. Информация, записанная в файл

Для записи в файл результата команды необходимо ввести в консоль следующую конструкцию: “ команда >> имя файла “. Например: «date >> ULGU.txt».

Список команд, используемых при выполнении работ в терминале, представлен в таблице 1.

Таблица 1. Команды, вводимые в консоль

Команда	Описание
uname -a	Показать версию ядра Linux
clear	Очищение экрана терминала (консоли)

date	Показывает текущую дату и время
hostname	Показать сетевое имя компьютера
exit	Завершить сеанс текущего пользователя
pwd	Выводит текущий путь (в каком каталоге находится пользователь)
cd /home	Переход в директорию /home
ls	Выводит список файлов и каталогов по порядку
top	Информация в реальном времени о загруженных процессах, потребление ОЗУ
ifconfig eth0	Показать параметры сетевого интерфейса eth0
who	Показывает имя текущего пользователя и время входа
mc	Переход в Midnight Commander (просмотр каталогов)
touch «имя файла»	Создание файла с именем «имя файла» в текущем каталоге
echo «информация» >> «имя файла»	Вводит в конец указанного файла информацию
cat «имя файла»	Просмотр файла, если файл создан; либо создание файла, если в текущем каталоге нет файла с таким именем

Приложение 4. Создание абонента и настройка маршрутизации в IP PBX Asterisk

Для создания абонента и настройки маршрутизации в IP PBX Asterisk необходимо изменить настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`. Для этого зайти в консоль на рабочем столе «Управление Asterisk CLI» (приложение 3).

Алгоритм выполнения работы:

1. Открыть для редактирования файл `/etc/asterisk/sip.conf` и добавить двух абонентов с номерами 10400 и 10401 (1VV00 и 1VV01, где VV это номер РМ, например, РМ4 имеет номер 04). Пример содержимого файла:

sip.conf (шаблон)

```
[general]
allowguest=no
udpbindaddr=172.16.119.Z
transport=udp
srvlookup=yes
disallow = all
allow = alaw
allow = ulaw
```

```
[172.16.119.X](!)
type=friend
host=dynamic
context= internal
disallow = all
allow = alaw
```

```
[1VV00](172.16.119.X)
[1VV01](172.16.119.X)
```

sip.conf (PM1)

```
[general]
allowguest=no
udpbindaddr=172.16.119.154
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
```

```
[172.16.119.4](!)
type=friend
host=dynamic
context=internal
disallow=all
allow=alaw
```

```
[10400](172.16.119.4)
[10401](172.16.119.4)
```

В шаблоне файла `sip.conf` вместо символов X прописывается последнее число IP-адреса РМ; V – цифры, обозначающие номера РМ; Z – последнее число адреса РМ на сервере Asterisk.

2. В файлы `/etc/asterisk/extensions.conf` добавить правила обработки вызовов:

extensions.conf (шаблон):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
exten => 1VV00,1,Dial(SIP/${EXTEN})
exten => 1VV00,n,Hangup()
exten => 1VV01,1, Dial(SIP/${EXTEN})
exten => 1VV01,n,Hangup()
```

extensions.conf (PM4):

```
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no
[internal]
```

```

exten => 10400,1,Dial(SIP/${EXTEN})
exten => 10400,n,Hangup()
exten => 10401,1,Dial(SIP/${EXTEN})
exten => 10401,n,Hangup()

```

В шаблоне файла *extensions.conf* вместо символов VV прописываются цифры, обозначающие номера РМ.

Пояснения к записям в конфигурационных файлах находятся в приложении 6.

3. Перезапустить процесс *asterisk* командой */etc/init.d/asterisk restart* (рис. 1).

4. С помощью команды *asterisk -rvvv* подключиться к консоли управления Asterisk (рис. 1).

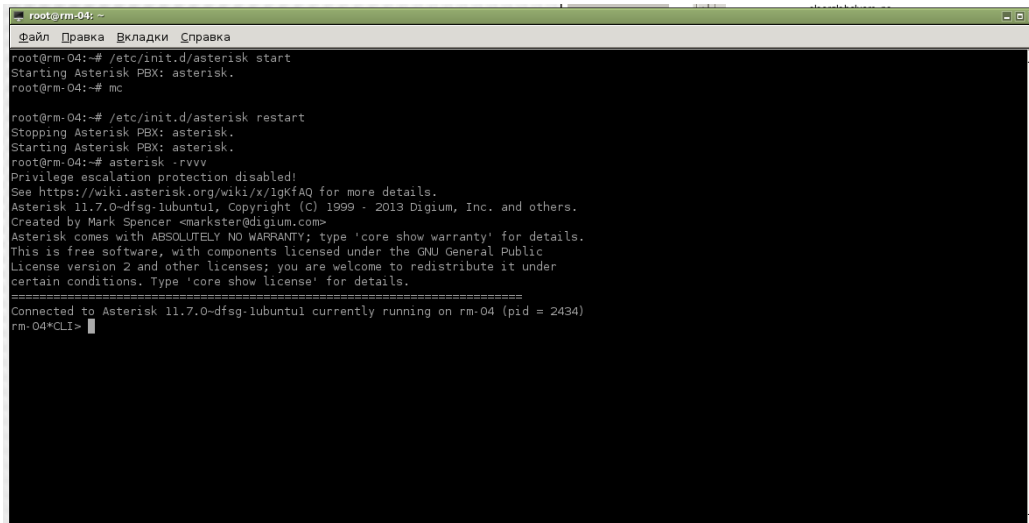


Рис. 1. Консоль управления Asterisk

5. На РМ запустить программный телефон Linphone. В настройках на вкладке «Настройки сети» изменить порт *UDP 5062*, на вкладке «Управление учетными записями SIP» добавить учетную запись с номером 10400 (1VV00). После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента (приложение 2). Пример записи об успешной регистрации абонента представлен на рис. 2.

6. На РМ запустить программный телефон Twinkle. В мастере создания учетных записей указать номер 10401 (1VV01). В системных настройках определить SIP порт 5063. После настройки программного телефона в консоли управления Asterisk появится запись об успешной регистрации абонента (приложение 1). Пример записи об успешной регистрации абонента представлен на рис. 2.

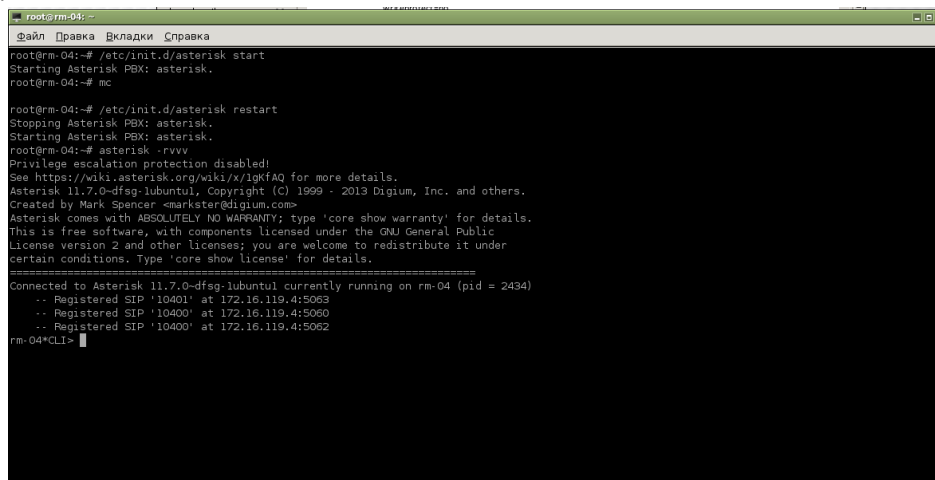


Рис. 2. Записи об успешной регистрации абонентов

7. Выполнить контрольный вызов между абонентами 10400 и 10401 (1VV00 и 1VV01) (рис. 3). В консоли управления Asterisk будут отображаться сообщения о ходе выполнения обработки

вызова. Успешный вызов свидетельствует о корректной настройке учетных записей абонентов и маршрутизации (рис. 4). Выход из консоли управления Asterisk осуществляется командой `exit`.

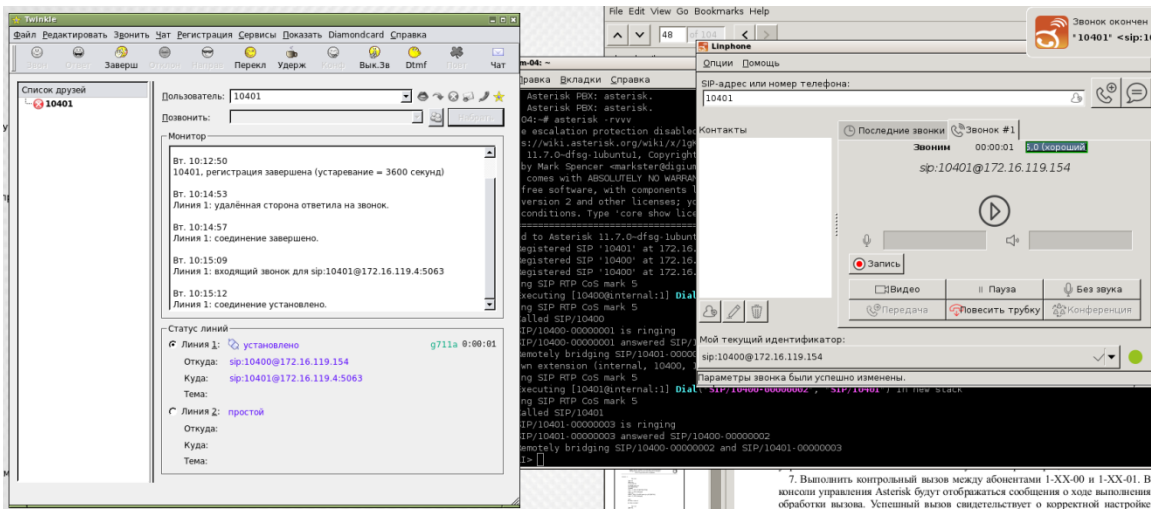


Рис. 3. Контрольный вызов между абонентами 10400 и 10401

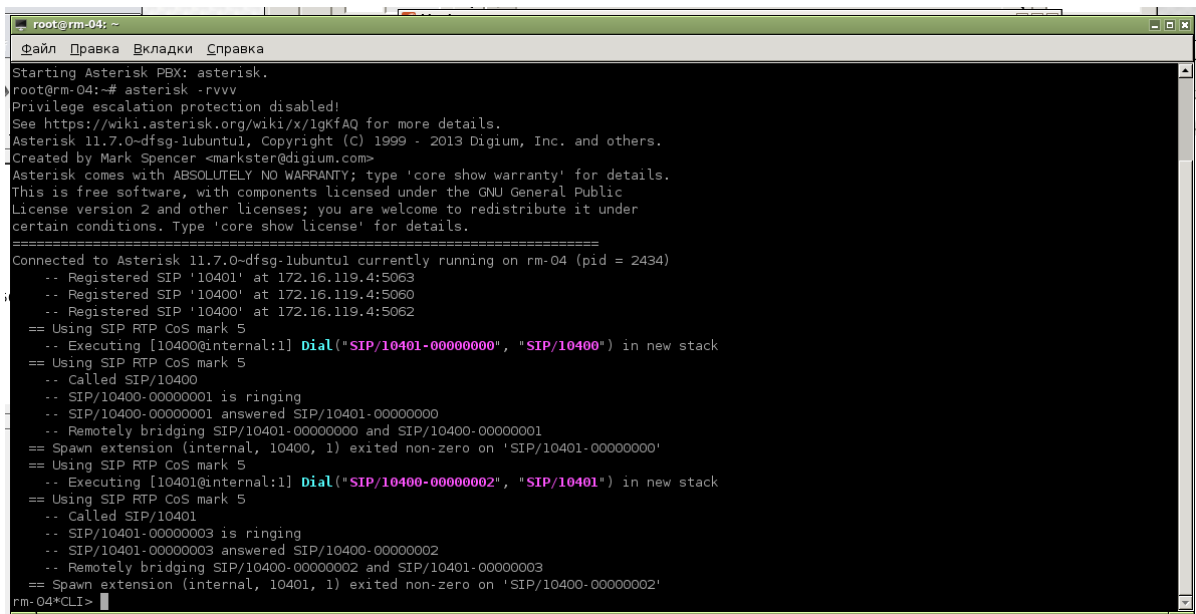


Рис. 4. Сообщения о ходе выполнения обработки вызовов

Приложение 5. Настройка аудио выхода.

- 1. Открыть программу по настройке звука, дважды нажав на иконку «Настройка звука» на рабочем столе.
- 2. В открывшемся окне выбрать подменю «Input». Изменить положение бегунка, на необходимый уровень, исходя от слышимости (рис.1).

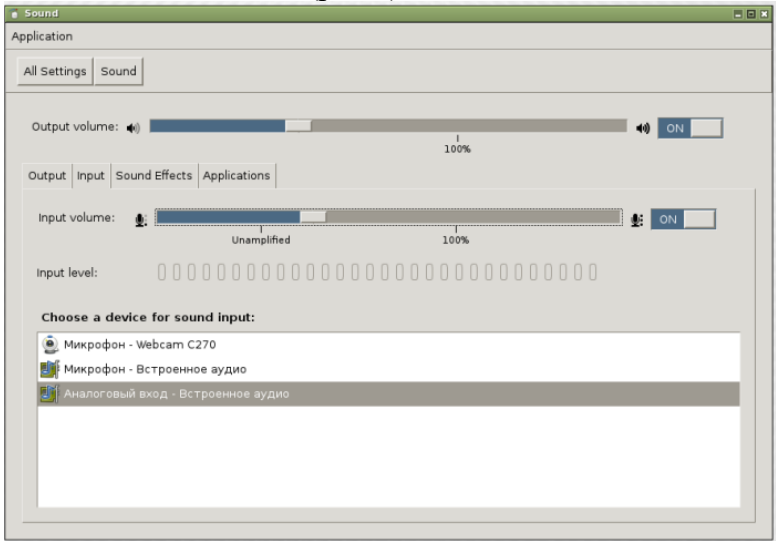


Рис. 1. Настройка звука (input)

- 3. В открывшемся окне выбрать подменю «Output». Изменить положение бегунка, на необходимый уровень, исходя от слышимости (рис.2).

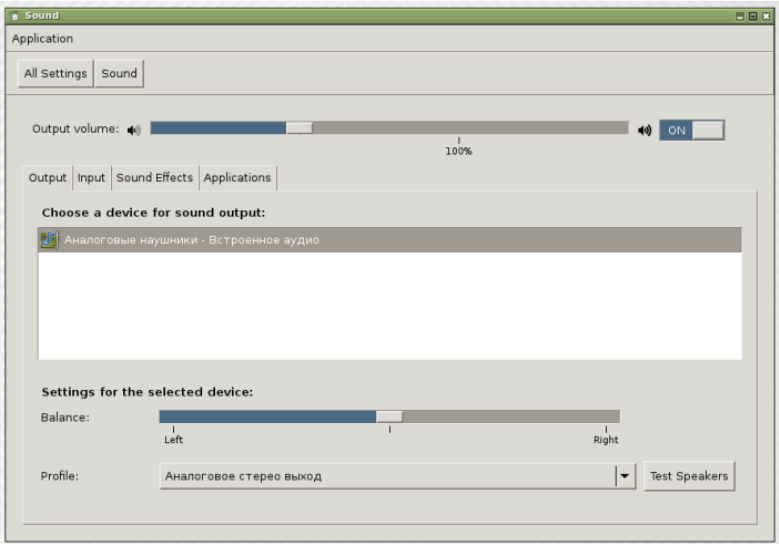


Рис. 2. Настройка звука (output)

Приложение 6. Содержимое файлов конфигурации с пояснениями

IP PBX Asterisk, как и большинство приложений, работает с использованием конфигурационных файлов. Изменению подвергаются настройки, хранящиеся в файлах `/etc/asterisk/sip.conf` и `/etc/asterisk/extensions.conf`.

Файл `sip.conf` содержит описание базовых параметров работы протокола SIP, настройки NAT, перечень используемых кодеков, учетных записей абонентов и т.д.

Файл `extensions.conf` описывает правила обработки вызовов поступающих в систему.

Содержимое файлов:

1. Файл `/etc/asterisk/sip.conf` (курсивом выделены поля, зависящие от номера РМ):

<code>[general]</code>	
<code>allowguest=no</code>	= запрещает гостевые вызовы
<code>udpbindaddr=172.16.119.160</code>	= указывает, на каком сетевом интерфейсе принимать UDP запросы (в данном случае UDP запросы будут приниматься на сетевом интерфейсе eth0:0)
<code>transport=udp</code>	= задает протокол транспортного уровня для сигнализации SIP (tcp или udp)
<code>srvlookup=yes</code>	= включает DNS поиск для вызовов
<code>disallow=all</code>	= запрещает использование всех кодеков (глобальная настройка)
<code>allow=alaw</code>	= определяет разрешенные кодеки, порядок
<code>allow=ulaw</code>	выбора кодака задается порядком их описания (сначала alaw, потом ulaw)
 <code>[sip_sub](!)</code>	= описывает клиентов SIP
<code>type=friend</code>	= содержит информацию о типе клиента: только исходящие вызовы (peer), только входящий (user) или все вместе (friend)
<code>host=dynamic</code>	= определяет IP адрес или имя хоста. Значение dynamic используется вместо IP адреса или имени хоста, чтобы телефон регистрировался самостоятельно.
<code>context=internal</code>	= определяет контекст плана набора, в который попадают вызовы, поступающие от данного абонента
<code>disallow=all</code>	= запрещает использование всех кодеков (глобальная настройка)
<code>allow=alaw</code>	= определяет разрешенные кодеки (единственный разрешенный кодек alaw)
 <code>[11000](sip_sub)</code>	= номер клиента SIP
<code>[11001](sip_sub)</code>	= номер клиента SIP

```

sip.conf [----]
[general]
allowguest=no
udpbindaddr=172.16.119.160
transport=udp
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw

[sip_sub](!)
type=friend
host=dynamic
context=internal
disallow=all
allow=alaw

[11000](sip_sub)
[11001](sip_sub)

```

Рис. 1. Пример изменения файла *sip.conf*

Вместо конструкции «*sip_sub*» прописывается IP РМ на которой происходит работа. Например на РМ10 прописывается *172.16.119.10*.

2. Файл */etc/asterisk/extensions.conf* (рис. 2):

[general]	
static=yes	= используется в паре со следующим параметром и необходим для настройки команды сохранения диалплана
writeprotect=no	= при установке <i>writeprotect=no</i> и <i>static=yes</i> появляется возможность сохранить текущий диалплан командой « <i>save dialplan</i> »
autofallthrough=yes	= при отсутствии явно указанных инструкций вызов завершится с значениями <i>BUSY</i> , <i>CONGESTION</i> или <i>HANGUP</i>
clearglobalvars=no	= глобальные переменные будут сохраняться при перезагрузках даже после удаления переменных из <i>extensions.conf</i> или других файлов
[internal]	= описание контекста <i>internal</i>
exten => 11000,1,Dial(SIP/\${EXTEN})	
exten => 11000,n,Hangup()	
exten => 11001,1,Dial(SIP/\${EXTEN})	
exten => 11001,n,Hangup()	

Контексты обозначаются как *[название_контекста]*. Структура контекста следующая:

exten => маска, порядок, действие
где:

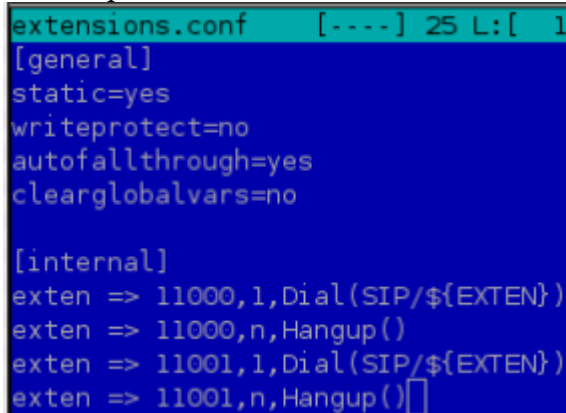
- exten => обозначает синтаксис добавочного номера;
- маска (имя добавочного номера) — маска номера, либо статически заданный номер;
- порядок (приоритет) — порядок действия для конкретной маски (возможна последовательность действий);
- действие — команда, выполняемая системой при попадании вызова на данное правило.

Каждый приоритет пронумерован последовательно, начиная с 1, и выполняет одно определенное приложение.

Например, здесь каждый добавочный номер отвечает на звонок (в приоритете под номером 1) и затем выполняет разъединение со значением *HANGUP* (в приоритете под номером n, который означает "следующий").

Команда *Dial(SIP/\${EXTEN})* нужна для осуществления вызова между разными абонентами. В аргументе прописывается название технологии или транспортного протокола, с помощью которого выполняется вызов, символ слэш и имени удаленной конечной точки или ресурса. В данном случае в *(SIP/\${EXTEN})* используется протокол *SIP* и переменная канала *\${EXTEN}* (При каждом звонке на добавочный номер Asterisk сохраняет набранный номер в переменной канала *\${EXTEN}*).

Команда *Hangup()* нужна для разъединения активного канала.



```
extensions.conf    [----] 25 L: [ 1
[general]
static=yes
writeprotect=no
autofallthrough=yes
clearglobalvars=no

[internal]
exten => 11000,1,Dial(SIP/${EXTEN})
exten => 11000,n,Hangup()
exten => 11001,1,Dial(SIP/${EXTEN})
exten => 11001,n,Hangup()
```

Рис. 2. Пример изменения файла *extensions.conf*.

Список информационных источников.

1. Бакланов И.Г. NGN: принципы построения и организации. – М.: Эко-Трендз, 2017. – 400 с.
2. Сети следующего поколения NGN / Под ред. А.В. Рослякова. – М.: Эко-Трендз, 2016. – 424 с.
3. Олифер В.Г. Основы компьютерных сетей / В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2015. -520 с.
4. Олифер В.Г. Компьютерные сети. Принципы, технологии, протоколы. 3-е изд./ В.Г. Олифер, Н.А. Олифер. - СПб.: Питер, 2016. - 958 с.
5. Пескова С.А. Сети и телекоммуникации 4-е изд., стер / С.А Пескова. - М.: Академия, 2015. - 350 с.
6. Абилов А.В. Сети связи и системы коммутации / А.В. Абилов. - М.: Радио и связь, 2015. - 288 с.
7. Гольдштейн Б.С. Softswitch / Б.С. Гольдштейн. - М.: БХВ - Санкт-Петербург, 2016. - 314 с.
8. Довгий С.А. Современные телекоммуникации / С.А. Довгий. - М.: Эко - Трендз, 2015. - 320 с.
9. Берлин А.Н. Коммутация в системах и сетях связи / А.Н. Берлин. - М.: Эко -Трендз, 2016. - 344 с.
10. Методическое пособие СОТСБИ-ngn. Преподаватель. Лабораторные и исследовательские работы по курсу «NGN. Протоколы IP- телефонии» / ООО «НТЦ СОТСБИ», 2016. – 104 с.
11. Руководство пользователя СОТСБИ-ngn. Преподаватель / ООО «НТЦ СОТСБИ», 2016. – 120 с.
12. Меггелен Дж., Мадсен Л., Смит Дж. Asterisk: будущее телефонии, второе издание. - Пер. с англ. - СПб Символ-Плюс, 2009. – 347 с.
13. Гольдштейн, Б. С. IP телефония - М.: Радио и связь, 2001. – 336 с.
14. Гольдштейн Б.С., Гойхман В.Ю., Столповская Ю.В. Сетевые анализаторы IP сетей. Учебное пособие. — СПб.: СПбГУТ, 2014. — 58 с.
15. Форум Asterisk [Электронный ресурс]. – URL: <http://forum.asterisk.ru>, свободный. –загл. с экрана. – Рус.,англ. (дата обращения: 12.09.2018)
16. Сайт Asterisk [Электронный ресурс]. – URL:<http://asterisk.org>, свободный. –загл. с экрана. – Рус.,англ. (дата обращения: 12.09.2018)
17. RFC 3261 SIP: Session Initiation Protocol J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. —The Internet Society, —2002.
18. Гольдштейн Б.С. Сети NGN. Оборудование IMS: учебное пособие. / Б.С. Гольдштейн Гойхман В.Ю., Сибирякова Н.Г., Столповская Ю.В. - СПбГУТ. —СПб —2010.
19. Гольдштейн Б.С. Протокол SIP. Справочник/ Б.С. Гольдштейн, А.А. Зарубин, В.В. Саморезов. —СПб.: БХВ —Санкт-Петербург, 2005. —456 с., ил.
20. Гольдштейн Б.С. Протокол SIP: учебное пособие для практических занятий и лабораторных работ/ Б.С. Гольдштейн, В.Ю. Гойхман, Д.Н. Онучина. —СПбГУТ; —СПб. —2008.