

ФЕДЕРАЛЬНОЕ АГЕНТСТВО СВЯЗИ

**Федеральное государственное бюджетное образовательное
учреждение высшего образования
«САНКТ-ПЕТЕРБУРГСКИЙ
ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТЕЛЕКОММУНИКАЦИЙ
им. проф. М. А. БОНЧ-БРУЕВИЧА»
(СПбГУТ)**

С. С. Владимиров

**ТЕХНОЛОГИИ АБОНЕНТСКОГО
ДОСТУПА В РАСПРЕДЕЛЕННЫХ
СЕТЯХ ПЕРЕДАЧИ ДАННЫХ**

Лабораторный практикум

СПб ГУТ)))

**Санкт-Петербург
2018**

УДК XXX.XXX.X (XXX)
ББК XX.XX хХХ
Х ХХ

Рецензенты

— —

*Утверждено редакционно-издательским советом СПбГУТ
в качестве учебного пособия*

Владимиров, С. С.

Х ХХ Технологии абонентского доступа в распределенных СПД : лабораторный практикум / С. С. Владимиров ; СПбГУТ. — СПб, 2018. — 38 с.

Учебное пособие призвано ознакомить студентов старших курсов с теорией абонентского доступа. Представленный материал служит справочным и методическим пособием при выполнении курса лабораторных работ по дисциплине «Технологии абонентского доступа в распределенных СПД».

Предназначено для студентов, обучающихся по направлениям 11.03.02 (210700.62) «Инфокоммуникационные технологии и системы связи», 09.03.01 (230100.62) «Информатика и вычислительная техника» и 09.03.04 (231000.62) «Программная инженерия».

**УДК XXX.XXX.X (XXX)
ББК XX.XX хХХ**

- © Владимиров С. С., 2018
- © Федеральное государственное бюджетное образовательное учреждение высшего образования «Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича», 2018

Содержание

Лабораторная работа 1. Ознакомление с программой xDSLcalc	4
1.1. Задание	4
1.2. Теоретические сведения	4
1.3. Порядок выполнения лабораторной работы	7
1.4. Контрольные вопросы	10
Лабораторная работа 2. Организация соединения между SHDSL-модемами	11
2.1. Задание	11
2.2. Теоретические сведения	11
2.3. Порядок выполнения лабораторной работы	13
2.4. Контрольные вопросы	15
Лабораторная работа 3. Организация абонентского доступа к услугам передачи речевой информации	16
3.1. Цель работы	16
3.2. Теоретические сведения	16
3.3. Порядок выполнения лабораторной работы	25
3.4. Контрольные вопросы	28
Лабораторная работа 4. Соединение узлов абонентского доступа через транзитный узел связи	29
4.1. Цель работы	29
4.2. Теоретические сведения	29
4.3. Порядок выполнения лабораторной работы	35
4.4. Контрольные вопросы	37

Лабораторная работа 1

Ознакомление с программой xDSLcalc

1.1. Задание

Ознакомиться с назначением и основами работы с программой xDSLcalc.

1.2. Теоретические сведения

1.2.1. Описание программы «xDSLcalc»

Программа «xDSLcalc» обеспечивает расчет скоростных характеристик цифровых абонентских линий ADSL, ADSL2, ADSL2+, VDSL2, VDSL2 vectoring и SHDSL, реализуемых на различных кабелях (как традиционных, так и цифровых новых конструкций) при разных вариантах их загрузки. Она позволяет проанализировать различные варианты построения сетей доступа; сопоставить скоростные характеристики линий xDSL различных типов и частотных планов. Одной из задач при ее разработке ставилось обеспечение возможности преобразования данные TV на кабели в радиусы зон гарантированного обслуживания технологий xDSL на заданной скорости. Программа разработана специалистами ООО «Аналитик-ТС» и НПП «Информсистема». Предназначена для ОС семейства MS Windows. В ОС семейства Linux запускается с использованием системы Wine.

Программа «xDSLcalc» позволяет построить графики зависимости скорости передачи данных от длины линии при задании следующих параметров:

1. Тип кабеля.
 - а) ЗКП 1x4x1,2 (предназначен для кабельных линий зоновой связи)
 - б) КСПП 1x4x0,9 и 1x4x1,2 (предназначены для линий межстанционной и абонентской связи сельских телефонных сетей)
 - в) МКС Nx4x1,2 (применяется на междугородных кабельных магистралях и соединительных линиях ГТС)
 - г) ТПП Nx2x0,4 и Nx2x0,5 (предназначен для эксплуатации в местных первичных сетях связи как абонентский кабель)
 - д) ТЦП Nx2x0,5; Nx2x0,52; Nx2x0,64 и Nx2x0,9 (применяется при протягивании абонентских линий телефонной связи внутри помещений и зданий)
2. Емкость M пучка кабеля (пар).
3. Загрузка t пучка кабеля (число линий xDSL).
4. Нормы ELFEXT для 1 км. Может быть задана частота нормы в кГц и набор возможных значений нормы в дБ.
5. Диапазон и шаг изменения длины кабеля.
6. Тип линии xDSL.

- а) ADSL Annex A и Annex B
 - б) ADSL2 Annex A и Annex B
 - в) ADSL2+ Annex A и Annex B
 - г) SHDSL (TC-PAM4, TC-PAM8, TC-PAM16, TC-PAM32, TC-PAM64)
 - д) VDSL2 (профили 8a, 12a, 17a, 30a)
7. Запас помехозащищенности SNR Margin
8. Шаблон помех на входе приемника. От -90 до -160 дБм на Гц с шагом 10.

При этом можно одновременно построить до 10 графиков, отличающихся одним из параметров (верно не для всех параметров).

Главное окно программы показано на рис. 1.1.

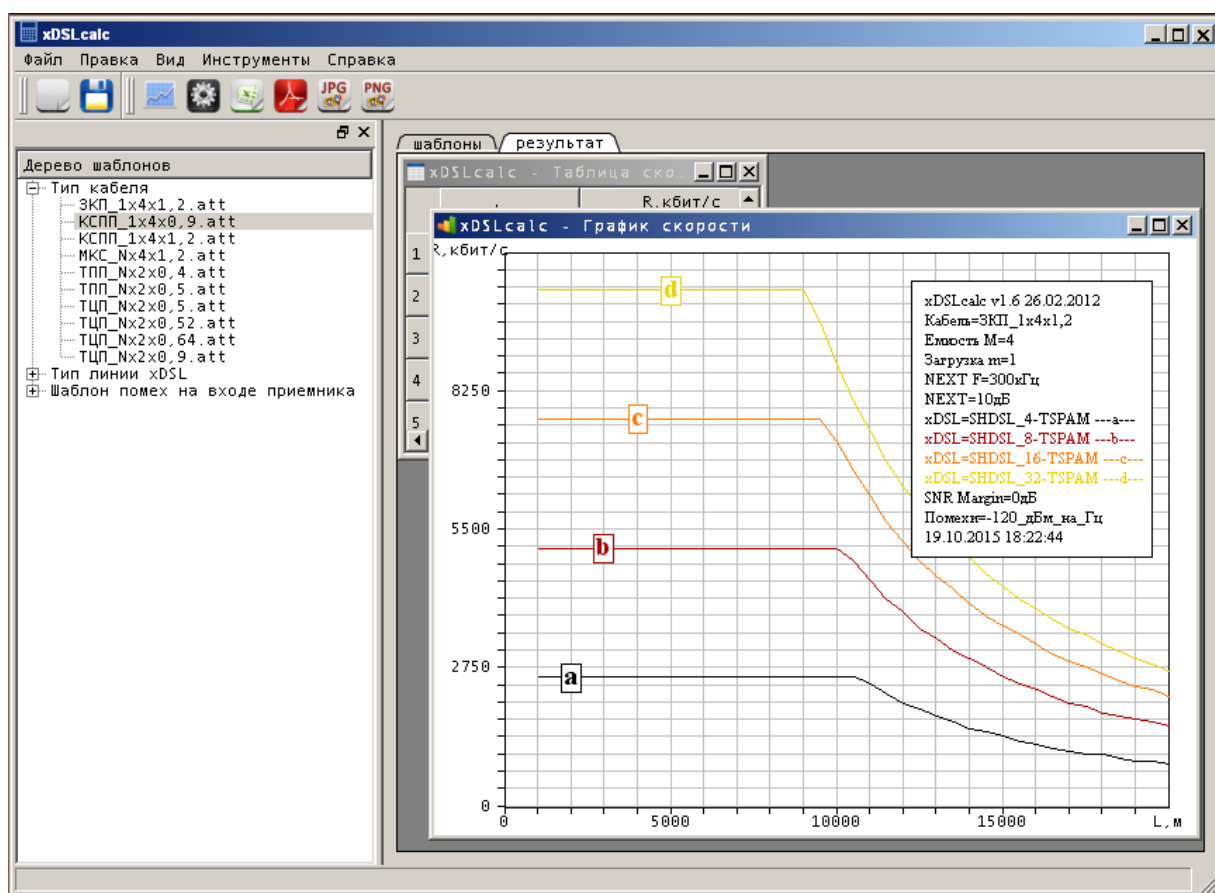


Рис. 1.1. Главное окно программы xDSLcalc

На рис. 1.2 показано окно ввода исходных данных. Оно вызывается по нажатию клавиши «F5» или при выборе пункта меню «Инструменты»—«Ввод исходных данных». На рис. 1.2 в качестве примера приведены исходные данные, соответствующие приведенным на рис. 1.1 графикам.

Построенные графики могут быть экспортированы в форматы PDF, JPG и PNG с помощью соответствующих пунктов подменю «Инструменты»—«График», а также одноименных кнопок на панели инструментов программы.

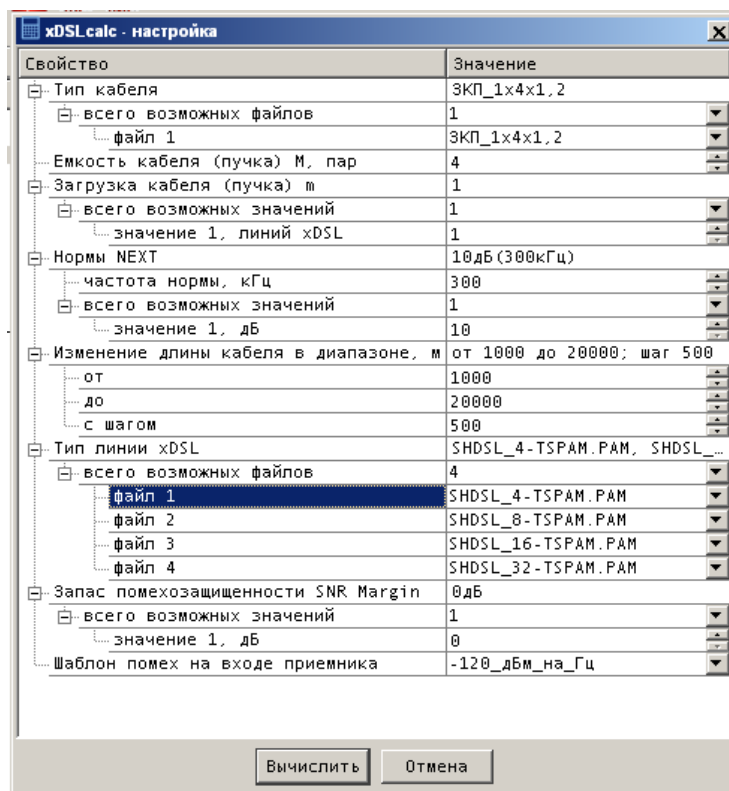


Рис. 1.2. Окно ввода исходных данных для построения графиков в программе xDSLcalc

Таблица значений, по которым строятся графики, может быть экспортирована в формат CSV (простая таблица MS Excel/LO Calc) с помощью соответствующего пункта подменю «Инструменты»—«Таблица», а также одноименной кнопки на панели инструментов программы.

Пункт меню «Инструменты»—«График»—«Настройки» (клавиша «F6» и одноименная кнопка на панели инструментов программы) вызывает окно настроек отрисовки графика, показанное на рис. 1.3.

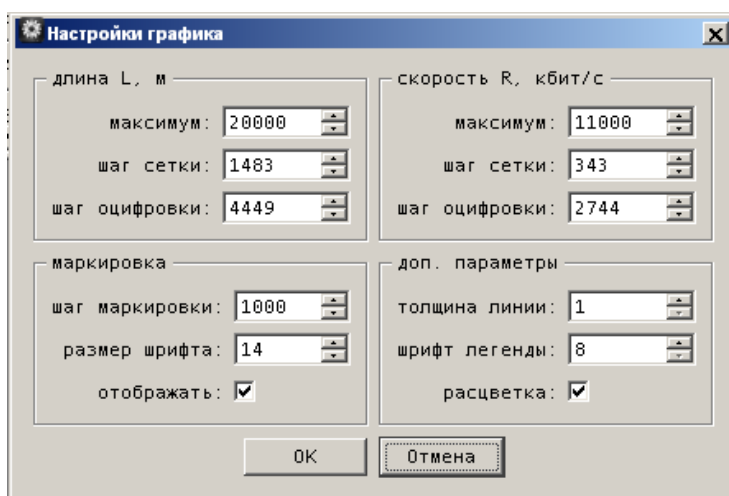


Рис. 1.3. Окно настроек отрисовки графика в программе xDSLcalc

1.2.2. Запуск «xDSLcalc»

На лабораторных компьютерах программа «xDSLcalc» запускается из главного меню.

«Главное меню» — «Эмуляторы сетевых устройств» — «xDSLcalc»

Также программа может быть скачана с официального сайта разработчика и запущена на личных ноутбуках учащихся.

<http://www.analytic.ru/products/6/soft/>

Список использованных источников

1. А.Кочеров, В.Руденко, А.Ковальчук. Сети и линии доступа — моделируй вместе с xDSLcalc // Первая миля. №5. 2011 г.

1.3. Порядок выполнения лабораторной работы

1. Построить графики зависимостей скорости передачи данных от расстояния передачи для исходных данных, заданных в пункте 1.3.1. Если какие-то из параметров не заданы явно, то используется предустановленное значение «по умолчанию». Если полученные графики являются неинформативными, то необходимо изменить (увеличить или уменьшить) изменение и шаг изменения длины кабеля, а также, возможно, изменить настройки отображения графика.

2. Сохранить таблицу значений для отчета.

Место для сохранения файлов: «Мой компьютер» — «Диск Z» — «home» — «student»

3. Сохранить графики для отчета.

4. Проанализировать графики и таблицу значений. Сделать выводы. Выводы (а также таблица и графики) должны быть внесены в отчет по работе.

5. Сравнить полученные результаты с табличными значениями скоростей передачи данных заданных технологий xDSL, приведенными в открытых источниках. Сделать выводы. Выводы должны быть внесены в отчет по работе.

1.3.1. Варианты для выполнения лабораторной работы

Варианты указаны в соответствии с номером студента в журнале.

1. Тип кабеля: ЗКП 1x4x1,2. Тип линии xDSL: SHDSL TC-PAM4; TC-PAM8; TC-PAM16; TC-PAM32; TC-PAM64. Шаблон помех на входе приемника: SHDSL.

2. Тип кабеля: МКС Nx4x1,2. Тип линии xDSL: ADSL Annex A и Annex B; ADSL2 Annex A и Annex B; ADSL2+ Annex A и Annex B. Шаблон помех на входе приемника: –120 дБм на Гц.

3. Тип кабеля: ТЦП Nx2x0,5; Nx2x0,52; Nx2x0,64 и Nx2x0,9. Тип линии xDSL: ADSL2+ Annex A. Шаблон помех на входе приемника: –120 дБм на Гц.
4. Тип кабеля: КСПП 1x4x1,2. Тип линии xDSL: ADSL2+ Annex A. SNR Margin: 0 дБ; 1 дБ; 23 дБ; 30 дБ. Шаблон помех на входе приемника: –120 дБм на Гц.
5. Тип кабеля: ЗКП 1x4x1,2; КСПП 1x4x0,9 и 1x4x1,2; МКС Nx4x1,2. Тип линии xDSL: VDSL2 профиль 12a ds. Шаблон помех на входе приемника: –120 дБм на Гц.
6. Тип кабеля: КСПП 1x4x0,9. Тип линии xDSL: ADSL Annex A; ADSL2 Annex A; ADSL2+ Annex A; SHDSL TC-PAM16. Шаблон помех на входе приемника: –100 дБм на Гц.
7. Тип кабеля: ТЦП Nx2x0,64. Тип линии xDSL: SHDSL TC-PAM4. SNR Margin: 6 дБ; 12 дБ; 18 дБ; 24 дБ; 30 дБ. Шаблон помех на входе приемника: –100 дБм на Гц.
8. Тип кабеля: ЗКП 1x4x1,2; МКС Nx4x1,2; КСПП 1x4x1,2; ТПП Nx2x0,4; ТЦП Nx2x0,5. Тип линии xDSL: VDSL2 профиль 30a ds. Шаблон помех на входе приемника: –140 дБм на Гц.
9. Тип кабеля: ТЦП Nx2x0,9. Тип линии xDSL: SHDSL TC-PAM128. SNR Margin: 0 дБ; 5 дБ; 10 дБ; 20 дБ; 25 дБ; 30 дБ. Шаблон помех на входе приемника: –120 дБм на Гц.
10. Тип кабеля: ТПП Nx2x0,4. Тип линии xDSL: ADSL Annex B; ADSL2 Annex B; ADSL2+ Annex B; SHDSL TC-PAM4. Шаблон помех на входе приемника: –120 дБм на Гц.
11. Тип кабеля: ЗКП 1x4x1,2. Тип линии xDSL: VDSL2 профили 8a us; 12a us; 17a us; 30a us. Шаблон помех на входе приемника: –100 дБм на Гц.
12. Тип кабеля: ТПП Nx2x0,4 и Nx2x0,5; ТЦП Nx2x0,5; Nx2x0,64 и Nx2x0,9. Тип линии xDSL: SHDSL TC-PAM16. Шаблон помех на входе приемника: –80 дБм на Гц.
13. Тип кабеля: ТЦП Nx2x0,9. Тип линии xDSL: SHDSL TC-PAM32. SNR Margin: 6 дБ; 12 дБ; 18 дБ; 24 дБ; 30 дБ. Шаблон помех на входе приемника: SHDSL.
14. Тип кабеля: ТПП Nx2x0,5. Тип линии xDSL: ADSL2+ Annex A; ADSL2 Annex A; VDSL2 8a ds; SHDSL TC-PAM16 и TC-PAM32. Шаблон помех на входе приемника: –110 дБм на Гц.
15. Тип кабеля: ТЦП Nx2x0,52. Тип линии xDSL: ADSL2+ Annex B; ADSL2 Annex B; VDSL2 12a ds; SHDSL TC-PAM4 и TC-PAM8. Шаблон помех на входе приемника: –100 дБм на Гц.
16. Тип кабеля: ЗКП 1x4x1,2; КСПП 1x4x0,9 и 1x4x1,2; ТЦП Nx2x0,52 и Nx2x0,9. Тип линии xDSL: ADSL Annex A. Шаблон помех на входе приемника: –110 дБм на Гц.

17. Тип кабеля: ЗКП 1x4x1,2. Тип линии xDSL: ADSL2+ Annex A. SNR Margin: 0 дБ; 1 дБ; 2 дБ; 24 дБ; 30 дБ. Шаблон помех на входе приемника: SHDSL.

18. Тип кабеля: КСПП 1x4x1,2. Тип линии xDSL: ADSL2 Annex A; ADSL Annex A; VDSL2 30a ds; SHDSL TC-PAM64 и TC-PAM128. Шаблон помех на входе приемника: SHDSL.

19. Тип кабеля: ЗКП 1x4x1,2; КСПП 1x4x0,9 и 1x4x1,2; ТЦП Nx2x0,52 и Nx2x0,64. Тип линии xDSL: ADSL Annex A. Шаблон помех на входе приемника: SHDSL.

20. Тип кабеля: МКС Nx4x1,2. Тип линии xDSL: ADSL Annex B. SNR Margin: 0 дБ; 5 дБ; 8 дБ; 15 дБ; 20 дБ. Шаблон помех на входе приемника: –110 дБм на Гц.

21. Тип кабеля: КСПП 1x4x1,2. Тип линии xDSL: ADSL2 Annex B; ADSL Annex B; VDSL2 8a us; SHDSL TC-PAM16 и TC-PAM32. Шаблон помех на входе приемника: –150 дБм на Гц.

22. Тип кабеля: ЗКП 1x4x1,2; КСПП 1x4x1,2; МКС Nx4x1,2; ТЦП Nx2x0,52 и Nx2x0,64. Тип линии xDSL: SHDSL TC-PAM32. Шаблон помех на входе приемника: SHDSL.

23. Тип кабеля: МКС Nx4x1,2. Тип линии xDSL: SHDSL TC-PAM16. SNR Margin: 0 дБ; 5 дБ; 8 дБ; 15 дБ; 20 дБ. Шаблон помех на входе приемника: SHDSL.

24. Тип кабеля: КСПП 1x4x0,9. Тип линии xDSL: VDSL2 8a us и 12a us; SHDSL TC-PAM32; TC-PAM64 и TC-PAM128. Шаблон помех на входе приемника: –120 дБм на Гц.

25. Тип кабеля: ЗКП 1x4x1,2; КСПП 1x4x0,9; ТПП Nx2x0,5; ТЦП Nx2x0,52 и Nx2x0,64. Тип линии xDSL: VDSL2 17a us. Шаблон помех на входе приемника: –120 дБм на Гц.

26. Тип кабеля: МКС Nx4x1,2. Тип линии xDSL: SHDSL TC-PAM4. SNR Margin: 2 дБ; 6 дБ; 10 дБ; 15 дБ; 20 дБ. Шаблон помех на входе приемника: –90 дБм на Гц.

27. Тип кабеля: ЗКП 1x4x1,2. Тип линии xDSL: ADSL Annex A и Annex B; SHDSL TC-PAM4; TC-PAM8 и TC-PAM16. Шаблон помех на входе приемника: SHDSL.

28. Тип кабеля: ЗКП 1x4x1,2; КСПП 1x4x0,9; ТПП Nx2x0,5; ТЦП Nx2x0,52 и Nx2x0,64. Тип линии xDSL: VDSL2 8a us. Шаблон помех на входе приемника: –160 дБм на Гц.

29. Тип кабеля: МКС Nx4x1,2. Тип линии xDSL: VDSL2 17a us. SNR Margin: 7 дБ; 8 дБ; 10 дБ; 12 дБ; 16 дБ. Шаблон помех на входе приемника: –90 дБм на Гц.

30. Тип кабеля: ЗКП 1х4х1,2. Тип линии xDSL: ADSL Annex A и Annex B; SHDSL TC-PAM4; TC-PAM8 и TC-PAM16. Шаблон помех на входе приемника: –110 дБм на Гц.

1.4. Контрольные вопросы

1. Описание технологии ADSL.
2. Отличия между ADSL Annex A и Annex B.
3. Отличия между ADSL, ADSL2 и ADSL2+.
4. Описание технологии SHDSL.
5. Модуляция TC-PAM.
6. Описание технологии VDSL2.
7. Отличия между VDSL2 8a и 12a.

Лабораторная работа 2

Организация соединения между SHDSL-модемами

2.1. Задание

Ознакомиться с назначением SHDSL-модемов и основами работы с ними. Научиться настраивать мостовые соединения между сегментами локальной сети с использованием SHDSL-модемов на примере модулей сетевого окончания FG-PAM-SAN-4Eth.

2.2. Теоретические сведения

2.2.1. Технология SHDSL

SHDSL (Single-pair High-speed DSL), G.shdsl, ITU G.991.2 — одна из xDSL-технологий, обеспечивает симметричную дуплексную передачу данных сигнала по паре медных проводников. Используется преимущественно для соединения абонентов с узлом доступа провайдера (так называемая последняя миля). Была принята в 2001 году. Используется модуляция TC-PAM (Trellis Coded Pulse Amplitude Modulation).

По стандарту технология SHDSL обеспечивает симметричную дуплексную передачу данных со скоростями от 192 Кбит/с до 2,3 Мбит/с (с шагом в 8 Кбит/с) по одной паре проводов, или от 384 кбит/с до 4,6 Мбит/с.м. по двум парам. При использовании методов кодирования TC-PAM128 стало возможным повысить скорость передачи до 15,2 Мбит/сек по одной паре и до 30,4 Мбит/сек по двум парам соответственно. При максимальной скорости (для провода 0,4 мм) рабочая дальность составляет около 3,5 км, а при минимальной — свыше 6 км.

На рис. 2.1 приведена схема использования SHDSL-модемов для объединения двух территориально разнесенных участков локальной сети.

SHDSL-модемы, использующиеся для объединения сетей, построенных по технологии Ethernet, могут иметь два режима работы. Первый режим работы — «мостовой» (bridge). При этом обе объединяемые сети (и сами модемы) должны иметь одну и ту же адресацию, то есть принадлежать к одной IP-сети (с точки зрения адресов). Второй режим — режим маршрутизатора (router). В этом случае, каждый из модемов играет роль маршрутизатора/шлюза для «своей» сети. Адресация сетей может не совпадать. Такие модемы могут выполнять функции DHCP-сервера и межсетевого экрана (firewall).

В работе используются SHDSL-модемы FG-PAM-SAN-4Eth фирмы Nateks, показанные на рис. 2.2. Эти модемы могут работать только в режиме моста.

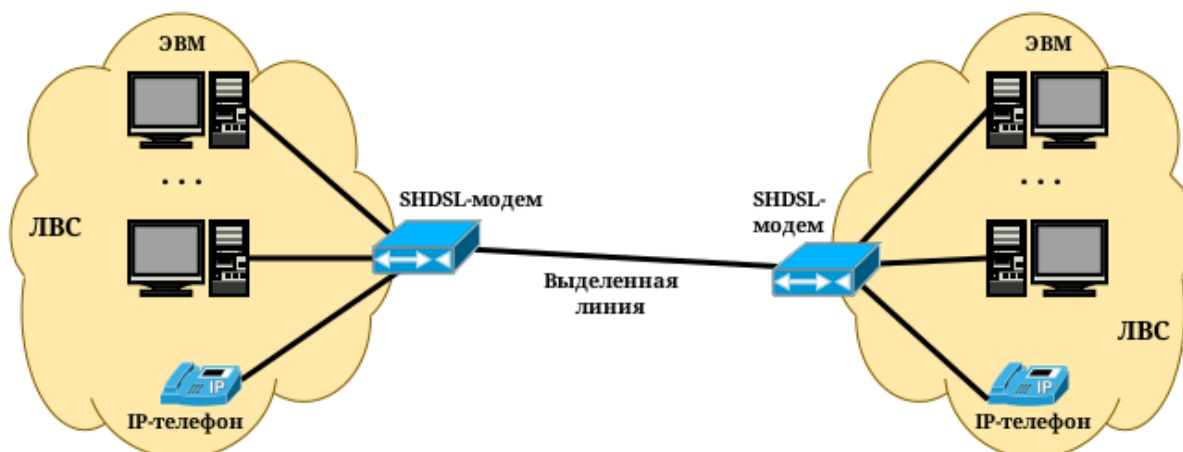


Рис. 2.1. Схема использования SHDSL-модемов для объединения территориально разнесенных участков локальной сети



Рис. 2.2. SHDSL-модемы FG-PAM-SAN-4Eth фирмы Nateks

2.2.2. Программа minicom для работы с последовательным портом

Minicom — это программа для работы с устройствами, подключающимися к ПК по последовательному порту. Аналог программы связи «Telix» в MS-DOS. Она эмулирует терминалы ANSI и VT102, имеет телефонную книгу и поддерживает основные протоколы передачи файлов для телефонных модемов. Программа предназначена для работы в эмуляторе терминала и имеет текстовый псевдооконный интерфейс на основе псевдографических символов.





Чтобы посмотреть подробное описание программы Minicom, необходимо в окне терминала ввести `man minicom`

Для запуска программы необходимо в окне терминала ввести команду `minicom`. Параметры программы могут быть указаны как опции командной строки либо настроены во внутреннем меню программы.

Пример запуска программы `minicom` в цветном режиме для подключения к устройству `/dev/ttyS1` со скоростью порта 115200 бит/с

```
minicom -c on -b 115200 -D /dev/ttyS1
```

Важно. После запуска программы настоятельно не рекомендуется изменять размер окна эмулятора терминала.

Для выхода из программы используется комбинация клавиш:  + , затем . После чего необходимо подтвердить выход нажатием клавиши .

Список использованных источников

1. Single-pair High-speed Digital Subscriber Line. Материал с сайта <https://ru.wikipedia.org>.
2. К. Изварский G.SHDSL — новый лидер. // «Экспресс-Электроника». № 5. 2004. Материал с сайта <http://citforum.ru>.
3. Оборудование линейного тракта серии FlexDSL FG-PAM-ALL-4Eth. Техническое описание и руководство по эксплуатации.
4. Minicom(1) — Linux man page. Материал с сайта <http://linux.die.net>.
5. Ю. Изотов Minicom — терминал на блюдечке. 2006. Материал с сайта <http://rus-linux.net>.

2.3. Порядок выполнения лабораторной работы

По выполнении работы должен быть подготовлен отчет, в котором должна быть представлена последовательность команд и результаты их работы.

1. Согласно заданию преподавателя выбрать первую или вторую пару SHDSL-модемов. Данные пар модемов приведены в табл. 2.1.

Таблица 2.1

Данные для подключения к SHDSL-модемам

Номер пары модемов	Номер модема	IP-адрес сервера	Имя пользователя	Пароль	Системное имя устр.
1	1	172.16.100.74	shdsl01	stud	/dev/ttyS0
	2	172.16.100.74	shdsl02	stud	/dev/ttyS1
2	1	172.16.100.74	shdsl03	stud	/dev/ttyS2
	2	172.16.100.74	shdsl04	stud	/dev/ttyS3

2. Открыть окно терминала и подключиться к удаленному стенду по протоколу SSH, используя учетные данные, соответствующие первому модему из выбранной пары.

Листинг 2.2

Пример команды подключения по SSH. IP-адрес 172.16.100.74. Пользователь shdsl01

```
ssh shdsl01@172.16.100.74
```

Далее потребуется ввести пароль. Сам пароль при вводе на экране отображаться не будет.

3. После подключения к стенду (сменится строка приглашения к вводу) запустить программу `minicom`, передав ей в качестве параметров скорость последовательного порта (9600 бит/с) и наименование модема в системе. Когда программа запустится, необходимо нажать клавишу «Enter», чтобы появилось приглашение командной строки модема (имеет вид: > >).

Листинг 2.3

Пример запуска программы minicom для подключения к модему /dev/ttyS4

```
minicom -c on -b 9600 -D /dev/ttyS4
```

4. Открыть второе окно терминала и подключиться к удаленному стенду по протоколу SSH, используя учетные данные, соответствующие второму модему из выбранной пары.

5. После подключения к стенду запустить программу `minicom`, передав ей в качестве параметров скорость последовательного порта и наименование модема в системе. Когда программа запустится, необходимо нажать клавишу «Enter», чтобы появилось приглашение командной строки модема.

6. Используя команды управления SHDSL-модемом, приведенные в руководстве, настроить для каждого из модемов IP-адрес и маску подсети. Для первого модема из пары: IP=192.168.1.1; Маска=255.255.255.0. Для второго модема из пары: IP=192.168.1.2; Маска=255.255.255.0. После настройки необходимо сохранить текущее состояние модема командой главного меню `save` (при этом модем будет перезагружен, что займет некоторое время).

- Команда главного меню `show` показывает текущие настройки Ethernet. Её вывод необходимо сохранить для отчета.
- Команда `setip` меню настроек Ethernet (1an) позволяет задать IP-адрес и маску подсети.

7. Используя команды управления SHDSL-модемом, приведенные в руководстве, настроить мостовое соединение между SHDSL-модемами. Для этого необходимо перейти в меню `sdsl`. Для просмотра установок используется команда `status`. Её вывод до начала настройки, после окончания настройки и после установления соединения надо сохранить для отчета. Когда настройки будут введены, их потребуется сохранить командой главного меню `save`. После установления соединения проверить его, использовав команду главного меню `ping`.

- Руководство по работе с модемами, представленное на сайте кафедры, предназначено как для модулей FG-PAM-SAN-4Eth (работают только в режиме моста (Bridge)) так и для модулей FG-PAM-SAN-4Eth-R (работают как в режиме моста (Bridge), так и в режиме роутера (Router)).

Соответственно, команды главного меню режима Router отсутствуют в модемах, используемых в лабораторной работе.

- При настройке DSL соединения между модулями сетевого окончания необходимо настроить один из модулей ведущим (COE), другой — ведомым (CPE) (команда `terminal`).
- Следующие настройки должны быть одинаковы на обоих модулях:
 - полярность битов данных в SDSL (команда `dbit`);
 - линейная скорость SDSL соединения (команда `rate`);
 - настройки скремблирования передаваемых ячеек ATM (команда `scramble`);
 - порядок передачи битов (команда `smbit`).
- Протокол Spanning Tree может быть как включен так и выключен.

8. Продемонстрировать факт установления соединения преподавателю.

9. Вернуть настройки в состояние «по-умолчанию». Команды главного меню модема

```
>> default
>> save
```

2.4. Контрольные вопросы

1. Описание технологии SHDSL.

Лабораторная работа 3

Организация абонентского доступа к услугам передачи речевой информации

3.1. Цель работы

Ознакомиться с принципами организации систем абонентского доступа к услугам передачи речевой информации на примере системы IP-телефонии, разворачиваемой на базе программной IP-АТС Asterisk.

3.2. Теоретические сведения

3.2.1. IP-АТС Asterisk

Asterisk представляет собой программную АТС IP-телефонии (IP-PBX — Internet Protocol Private Branch Exchange) с открытым исходным кодом. Разработкой Asterisk занимается компания Digium Inc., основанная Марком Спенсером. Работает на операционных системах Linux, BSD Unix, Solaris и др. Имя проекта произошло от названия символа «*» (англ. asterisk — «звёздочка»).

В ОС семейства GNU/Linux конфигурационные файлы Asterisk размещаются в каталоге

```
/etc/asterisk/
```

К основным конфигурационным файлам, используемым для базовой настройки Asterisk относятся:

- asterisk.conf — Asterisk берет из этого файла информацию о том, где хранятся все остальные файлы конфигурации;
- sip.conf — содержит настройки протокола SIP и абонентов, подключаемых по этому протоколу;
- iax.conf — содержит настройки протокола IAX2 и АТС, подключаемых по этому протоколу;
- extensions.conf — содержит настройки маршрутизации и обработки вызовов (план набора);
- extensions.ael — план набора в новом формате AEL (Asterisk Extensions Language);
- voicemail.conf — конфигурация голосовых почтовых ящиков;
- users.conf — настройка учетных записей пользователей; строго говоря, не является обязательным элементом, поскольку пользователей можно описать (и чаще всего так и делают) в файлах конфигурации соответствующих протоколов; считается, что использование этого файла обеспечивает большую простоту настройки Asterisk ценой немного меньшей гибкости.


3.2.1.1. Командная строка Asterisk

Для мониторинга и контроля параметров Asterisk при его настройке и работе удобно использовать встроенный интерфейс командной строки, запускаемый командой

```
# asterisk -r
```

Помимо результата выполнения команд Asterisk на экран будут выводиться служебные сообщения. Например, сообщения о регистрации и отключении пользователей.

Для более подробного вывода можно использовать флаг «-v».

При работе в командной строке Asterisk удобно использовать автодополнение по клавише  (табуляция).

Некоторые полезные команды и их краткое описание приведены в табл. 3.1.

Таблица 3.1

Команды для работы в командной строке Asterisk

Команда	Описание
sip show users	Отображает пользователей, прописанных в настройках SIP.
sip show peers	Отображает зарегистрировавшихся пользователей SIP.
iax2 show users	Отображает пользователей, прописанных в настройках IAX.
iax2 show registry	Отображает регистрацию пользователей IAX.

Asterisk позволяет работать с различными протоколами. Тем не менее, как правило используется следующая схема: для подключения абонентов используется протокол SIP, а для связи между отдельными IP-АТС или сетями IP-телефонии применяются либо каналы SIP-trunk, либо протокол IAX2 (обычно также «транковые» каналы).

В дальнейшем будем рассматривать следующий пример. Основная IP-АТС mainpbx, к которой по протоколу SIP подключаются абоненты с номерами 1001, 1002 и т. д. (имена абонентов, соответственно, User1001, User1002, ...). К основной АТС по протоколу IAX2 подключается вторая IP-АТС scndpbx, к которой по протоколу SIP подключаются абоненты с номерами 2001, 2002 и т. д. (имена абонентов, соответственно, User2001, User2002, ...).

3.2.1.2. Конфигурация протокола SIP (sip.conf)

При настройке Asterisk в конфигурационных файлах удобно использовать систему шаблонов. При этом вначале прописываются базовые шаблоны, которые затем можно наследовать в других шаблонах. Простой пример файла настройки sip.conf (для базовой АТС mainpbx) приведен ниже на листинге 3.1.

Простой пример файла настройки sip.conf

```
[general]
allowguest=no
allowoverlap=no
alwaysauthreject=yes
useragent=OPDSPBX
sdpsession=OPDS PBX
defaultexpiry=3600
limitonpeer=yes
rtptimeout=360
rtpholdtimeout=300
rtpkeepalive=5
language=ru
bindport=24060
bindaddr=192.168.1.2
externip=105.12.12.11
localnet=192.168.1.0/255.255.255.0
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
nat=yes
dtmfmode=info
canreinvite=no
insecure=invite

[default]
transport=udp

[friend](!,default)
type=friend
host=dynamic
qualify=yes

[local](!,friend)
context=localsip

[1001](local)
callerid=User1001
secret>Password1001
mailbox=1001
```

В приведенном файле используется следующая разбивка на шаблоны:

1. Шаблон **general**. Хранит основные настройки IP-АТС, касающиеся протокола SIP. В этом разделе указываются настройки всей АТС, а также настройки, касающиеся пользователей. Пользовательские настройки при этом могут быть переопределены в других шаблонах и даже указываться для конкретных пользователей.

2. Шаблон **default**. Базовый шаблон для пользователей.
3. Шаблон **friend**. Шаблон пользователей типа friend. Наследует шаблону default.
4. Шаблон **local**. Шаблон локальных пользователей, прописываемых в самой АТС. Наследует шаблону friend.
5. Шаблон **1001**. Пользователь (абонент) IP-АТС с номером 1001. Наследует шаблону local.

Краткое описание приведенных в примере параметров конфигурации файла sip.conf дано в табл. 3.2. Полный список возможных параметров и их подробное описание с примерами можно посмотреть в сетевых источниках и примере конфигурационного файла, поставляемого с исходным кодом Asterisk.

Таблица 3.2

Параметры конфигурации файла sip.conf

Параметр	Описание
allowguest	Определяет возможность подключения абонентов, не прописанных в конфигурации («гостей»). В целях безопасности рекомендуется запрещать доступ таким гостевым пользователям, явно присвоив параметру значение «no».
allowoverlap	Определяет возможность указания номеров с дополнительными цифрами. В целях безопасности рекомендуется отключить, явно присвоив параметру значение «no». Значение «yes» включает использование стандарта RFC3578. Значение «dtmf» обеспечивает использование стандарта RFC2833 и добавочных цифр при наборе номера в процессе его обработки.
alwaysauthreject	При включении параметра (значение «yes») все ошибки будут возвращаться клиенту как ошибки авторизации, что может затруднить взлом АТС. При настройке АТС параметр можно отключить (значение «no»).
useragent	Позволяет указать имя АТС.
sdpsession	Имя АТС, указываемое в сессии протокола SDP.
defaultexpiry	Время до перерегистрации абонента в секундах.
limitonpeer	Указывает считать исходящие и входящие вызовы пиров вместе (значение «yes»).
rtptimeout	Время в секундах до автоматического отбоя соединения при неактивности в голосовом канале.
rtpholdtimeout	Время до автоматического отбоя соединения при неактивности в голосовом канале в случае вызова, стоящего на удержании.
rtpkeepalive	Время в секундах между отправкой RTP-keepalive пакетов, необходимыми для поддержания открытой сессии NAT на маршрутизаторе.
language	Язык системы (голосовое меню, сообщения автоответа) по умолчанию. Этот параметр также можно определить отдельно для каждого пользователя или шаблона пользователей.

Параметры конфигурации файла *sip.conf*

Параметр	Описание
bindport	Определяет номер порта, на котором ожидается подключение SIP-клиентов. По умолчанию используется порт 5060. Использование другого порта увеличивает безопасность системы, но усложняет настройку клиентских приложений.
bindaddr	IP-адрес сетевого интерфейса, на котором АТС ожидает входящие подключения. Можно указать отдельные значения для протоколов UDP, TCP и TLS (параметры «udpbindaddr», «tcpbindaddr» и «tlsbindaddr», соответственно). Через двоеточие после адреса можно указать номер порта.
externip	Внешний IP-адрес. Используется, если АТС находится за NAT. Если АТС работает только в одном сегменте локальной сети, то указывается IP-адрес основного сетевого интерфейса АТС.
localnet	Адрес и маска сегмента локальной сети, в котором работает АТС.
srvlookup	Позволяет использовать SRV-записи DNS для исходящих звонков. Всегда используется первая SRV-запись в домене.
disallow	Позволяет отключить аудио-кодеки. Обычно отключают все аудио-кодеки, присвоив значение «all», а затем включают необходимые кодеки командой «allow». Параметры «disallow» и «allow» могут быть прописаны как для всей АТС, так и отдельно для каждого пользователя или шаблона пользователей.
allow	Активирует необходимые кодеки. Некоторые возможные значения: <ul style="list-style-type: none"> • «ulaw» — кодек G.711 (64 кбит/с, компандирование μ-law, североамериканский стандарт); • «alaw» — кодек G.711 (64 кбит/с, компандирование A-law, европейский стандарт); • «gsm» — кодек GSM (13 кбит/с); • «g729» — кодек G.729 (8 кбит/с, требует лицензии). Можно прописывать каждый кодек отдельным параметром, как в примере на листинге 3.1, а можно прописать все кодеки в одном параметре: «allow=!all,alaw,ulaw».
nat	Указывает необходимость использования NAT.
dtmfmode	Тип тонового набора. По умолчанию используется стандарт RFC2833 (значение «rfc2833»). Тем не менее в некоторых источниках рекомендуется явно указывать значение «info», для использование сообщений SIP INFO протокола SIP. Также можно указать значение «inband», т. е. передачу тоновых сигналов прямо в голосовом канале (используется только вместе с кодеком G.711).
canreinvite	Позволяет передавать аудиопоток напрямую между абонентскими терминалами, минуя сервер. Требуется, чтобы абоненты находились в одной сети (или имели «белые» IP-адреса), а также использовали одинаковый аудиокодек. Позволяет снизить нагрузку на АТС при соблюдении вышеуказанных условий. Параметр можно прописать как для всей АТС, так и отдельно для каждого пользователя или шаблона пользователей.

Параметры конфигурации файла *sip.conf*

Параметр	Описание
<code>insecure</code>	Отключает проверки: «invite» — не требует аутентификацию сообщений INVITE; «port» — контролирует только IP-адрес абонента, но не проверяет номер порта.
<code>transport</code>	Указывает используемый транспортный протокол («udp» или «tcp»).
<code>type</code>	Тип абонента: <ul style="list-style-type: none"> • «peer» — разрешены входящие и исходящие звонки; абоненты привязываются к IP-адресу и порту; • «user» — разрешены только входящие звонки (от пользователя к АТС); авторизация по логину/паролю (authname/secret); • «friend» — вариант пользователя «peer», требующий авторизацию. <p>Обычно используют тип «friend», как наиболее универсальный.</p>
<code>host</code>	Указывает IP-адрес абонента. Если значение равно «dynamic», то абонент может подключаться с любого IP-адреса. При этом исходящее соединение (к абоненту) возможно только после его регистрации.
<code>qualify</code>	Проверка доступности абонента. Раз в две секунды, если указано значение «yes». Также можно указать интервал проверки в миллисекундах.
<code>context</code>	Используемый план набора. Параметр можно прописать как для всей АТС, так и отдельно для каждого пользователя или шаблона пользователей.
<code>callerid</code>	Полный идентификатор абонента.
<code>secret</code>	Пароль абонента.
<code>mailbox</code>	Номер голосового почтового ящика абонента.

3.2.1.3. Конфигурация протокола IAX2 (*iax.conf*)

Протокол IAX2 (RFC 5456) используется для организации каналов между IP-АТС Asterisk и другими программными и аппаратными системами IP-телефонии, поддерживающими этот протокол. Существуют даже программные клиенты (софтфоны), поддерживающие этот протокол.

Протокол IAX2 использует один общий порт UDP (4569) для управляющего трафика и трафика данных, что обеспечивает более удобную работу через NAT по сравнению с соединением станций по SIP, где требуются дополнительные настройки (иногда на маршрутизаторе) в зависимости от сценария работы АТС.

Простой пример файла настройки *iax.conf* приведен ниже на листинге 3.2.

Листинг 3.2

Простой пример файла настройки *iax.conf*

```

[general]
autokill=yes

register => mainpbx:mainpassw@192.168.1.71

[scndpbx]
type=friend
host=dynamic
secret=scndpassw
trunk=yes
context=scndpbx_incoming
deny=0.0.0.0/0.0.0.0
permit=192.168.1.71/255.255.255.255

```

В данном примере приведена настройка протокола IAX на базовой АТС с учетной записью `mainpbx` и паролем `mainpassw`. К базовой АТС подключается вторая АТС `scndpbx`, размещенная на ЭВМ с IP-адресом 192.168.1.71. Видно, что на базовой АТС прописывается учетная запись второй АТС и команда `register` для автоматической регистрации на ней. Соответственно, на второй АТС должна быть аналогичным образом прописана учетная запись базовой АТС и соответствующая команда автоматической регистрации.

Краткое описание приведенных в примере параметров конфигурации файла `iax.conf` дано в табл. 3.3. Полный список возможных параметров и их подробное описание с примерами можно посмотреть в сетевых источниках и примере конфигурационного файла, поставляемого с исходным кодом Asterisk.

Таблица 3.3

Параметры конфигурации файла `iax.conf`

Параметр	Описание
<code>autokill</code>	Используется для авторазрыва соединений от не отвечающих узлов. Активация этой настройки может быть неудачным решением в случае использования нестабильных каналов связи.
<code>register</code>	Позволяет указать команду для автоматической регистрации на другой IP-АТС. При ее использовании параметр « <code>host</code> » необходимо установить динамическим (« <code>dynamic</code> »).
<code>host</code>	Указывает IP-адрес узла. Поскольку IP-АТС обычно имеют фиксированный адрес, в целях безопасности рекомендуется указывать конкретный адрес для каждой АТС. Тем не менее, как и при настройке клиентов SIP можно указать значение « <code>dynamic</code> ». Его использование может быть оправдано при настройке АТС или использовании мобильного выноса, который может перемещаться между различными сетями. Если IP-адрес задан, то команда « <code>register</code> » не используется.

Параметры конфигурации файла `iax.conf`

Параметр	Описание
trunk	Указывает рассматривать связь с прописываемым узлом как транк, разрешая организовывать несколько одновременных разговоров. Использование «транковой» связи позволяет немного улучшить качество связи на плохих каналах.
context	План набора, используемый для соединений, приходящих от абонентского выноса.
deny	Указывает с каких адресов нельзя принимать соединения. В примере на листинге 3.2 вначале запрещаются все адреса, а затем разрешается один конкретный IP-адрес.
permit	Указывает с каких адресов ожидать соединения от прописанного узла. Как правило указывается конкретный IP-адрес (кроме случаев мобильного выноса).

3.2.1.4. Настройка маршрутизации вызовов (`extensions.conf`)

Простой пример файла маршрутизации вызовов `extensions.conf` (для базовой АТС `mainpbx`) приведен ниже на листинге 3.3.

Листинг 3.3

Простой пример файла маршрутизации вызовов `extensions.conf`

```
[general]
static=yes
writeprotect=yes

[globals]

[macro-dial-sip]
exten => s,1,NoOp()
exten => s,n,Dial(SIP/${ARG1},20,tT)
exten => _s-. ,n,Hangup()

[macro-dial-iax]
exten => s,1,NoOp()
exten => s,n,Dial(IAX2/${ARG1})
exten => _s-. ,n,Hangup()

[default]

[incoming_calls]

[localsip]
include => internal
include => remote

[internal]
exten => _1XXX,1,Macro(dial-sip,${EXTEN})
exten => _User1XXX,1,Macro(dial-sip,${EXTEN:4})

[remote]
exten => _2XXX,1,Macro(dial-iax,mainpbx:mainpassw@scndpbx/${EXTEN})
```

```
[scndpbx_incoming]
include => internal
```

Данный пример соответствует ранее показанным примерам настроек SIP и IAX2.

В разделе `general` указываются общие параметры «`static`» и «`writprotect`», запрещающие изменение конфигурации из командной строки Asterisk.

Далее в разделе `globals` приводятся макросы, определяющие обработку звонков для протоколов SIP и IAX2. Структура обработки вызова простая: звонок по заданному номеру и отбой линии по завершении разговора или в случае неответа абонента.

В секции `default` добавлена секция `incoming_calls`, где определен контекст `localsip`, определяющий планы вызовов для локальных абонентов, подключенных к АТС. Видно, что для локальных абонентов доступны звонки согласно контексту `internal`, определяющему звонки по макросу `macro-dial-sip` на локальные номера по цифровому номеру и по идентификатору абонента. Также для них доступны вызовы согласно контексту `remote`, определяющему звонки по макросу `macro-dial-iax` на номера абонентов, подключенных к второй АТС `scndpbx`. Звонки также возможны по номеру и по идентификатору абонента.

Для входящих вызовов от второй АТС `scndpbx` (контекст `scndpbx_incoming`) доступен только контекст `internal`.

В случае второй АТС `scndpbx` план нумерации будет отличаться по нумерации. В контексте `internal` будут обрабатываться вызовы на номера [2001, ...] по макросу `macro-dial-sip`, а в контексте `remote` будут обрабатываться вызовы на номера [1001, ...] по макросу `macro-dial-iax` с ретрансляцией вызовов на базовую АТС `mainpbx`.

3.2.2. SIP клиент *Linphone*

Linphone — это программный SIP-клиент (софтфон) с открытым исходным кодом, разработанный компанией *Belledonne Communications*. Распространяется по лицензии GNU GPL. Существуют версии для основных десктопных ОС (MS Windows, Mac OS, GNU/Linux) и мобильных ОС (iOS, Android, BlackBerry). В ОС Linux используются графический интерфейс (GUI), основанный на GTK, и интерфейс командной строки (CLI).

Для подключения *Linphone* к IP АТС, необходимо прописать в настройках учетную запись абонента. Ниже приведена последовательность действий для графического интерфейса.

1. Пункт главного меню «Настройки» → «Параметры» → «Управление учетными записями SIP».

2. Нажать кнопку «Добавить». Появится окно «Настроить учетную запись SIP».

3. В окно внести:

- идентификатор SIP: sip:номер@IP-адрес-АТС;
- адрес SIP-прокси: <sip:IP-адрес-АТС>;
- маршрут: sip:IP-адрес-АТС;
- отметить пункт «Зарегистрироваться».

4. Нажать кнопку «ОК».

5. Нажать кнопку «Готово».

В случае успешной регистрации будет выведено сообщение в нижней части главного окна программы.

Для совершения звонка необходимо вписать номер или имя абонента в строку ввода и нажать кнопку вызова (зеленая кнопка справа от строки ввода номера).

3.2.3. Список использованных источников

1. Asterisk // Материал с сайта Wikipedia.org. URL: <https://ru.wikipedia.org/wiki/Asterisk>.

2. IAX // Материал с сайта Voip-info.org. URL: <https://www.voip-info.org/iax/>.

3. Asterisk SIP NAT solutions // Материал с сайта Voip-info.org. URL: <https://www.voip-info.org/asterisk-sip-nat-solutions/>.

4. Linphone open-source voip software // Материал с сайта Linphone.org. URL: <http://www.linphone.org/>.

5. Linphone // Материал с сайта Wikipedia.org. URL: <https://ru.wikipedia.org/wiki/Linphone>.

3.3. Порядок выполнения лабораторной работы

Лабораторная работа предназначена для выполнения двумя бригадами студентов не более двух человек каждая. Допускается выполнение на личных ноутбуках, в том случае, если обе бригады используют личные ноутбуки и эти ноутбуки способны запускать виртуальные машины.

По результатам работы должен быть сделан отчет. По каждому пункту должны быть указаны: команда и результат выполнения команды (в текстовом формате). По каждому подразделу должны быть сделаны и написаны выводы. Отчет должен быть оформлен в электронном виде в формате PDF и выслан на электронную почту преподавателя. Допускается также сдача печатного экземпляра отчета (в этом случае листы отчета не должны быть сшиты, допускается только скрепление листов на канцелярскую скрепку).

В результате работы необходимо настроить две IP-АТС Asterisk, на каждой из которых будет своя трехзначная нумерация абонентов, подключаемых по протоколу SIP, а затем соединить две АТС по протоколу IAX2. При этом необходимо обеспечить возможность звонков от абонентов одной АТС к абонентам второй АТС. Примерная схема сети IP-телефонии, которая должна быть реализована, приведена на рис. 3.1.

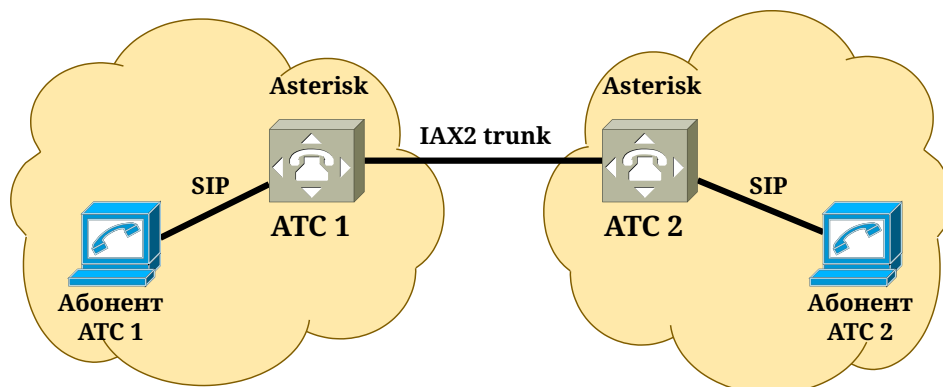


Рис. 3.1. Схема сети IP-телефонии, которую необходимо реализовать в лабораторной работе

АТС 1 и АТС 2 разворачиваются на виртуальной машине VirtualBox под управлением ОС OpenWRT Linux с предустановленным Asterisk. Архив tar.gz с образом ОС и файлами конфигурации VirtualBox размещен на сайте лаборатории. Содержимое архива (каталог «owrt-pbx») необходимо распаковать в каталог

```
/home/student/VirtualBox VMS /
```

Далее необходимо запустить VirtualBox и открыть в нем сохраненную виртуальную машину:

- пункт меню «Машина»;
- «Добавить»;
- выбрать каталог «owrt-pbx»;
- выбрать файл «owrt-pbx.vbox».

После этого в боковой панели появится ярлык виртуальной машины.

Виртуальная машина имеет имя «owrt-pbx». Перед началом работы необходимо клонировать эту виртуальную машину, назвав ее «РВХ-Номер группы-ФИО учащегося». Вместо «Номер группы» и «ФИО учащегося» транслитом указываются номер группы и ФИО учащегося, выполняющего работу. Например, «РВХ-ИКТХ-21-IvanovAS». Все настройки необходимо проводить на клонированной виртуальной машине. После завершения работы клонированная виртуальная машина не удаляется. Она будет использоваться в последующих работах. Каталог с образом необходимо сохранить на флешке или ином носителе.

Учетная запись пользователя IP-АТС:

- логин: root
- пароль: student

Каждая бригада настраивает одну АТС и минимум двух абонентов для проверки связи внутри АТС. При первом включении IP-АТС необходимо настроить IP-адрес. Для этого необходимо отредактировать конфигурационный файл командой

```
mcedit /etc/config/network
```

Требуемые сетевые настройки:

- IP-адрес: 172.16.101.xx, где xx берется таким же, как и последний байт IP-адреса хостовой машины;
- шлюз: 172.16.100.18;
- DNS-сервер: 172.16.4.13;
- маска подсети: 255.255.252.0.

После внесения изменений файл необходимо сохранить (клавиша F2) и закрыть (F10). Далее требуется перезагрузить виртуальную машину. После этого запущенная виртуальная машина должна быть видна в общей сети кафедры.

В дальнейшем настройку IP-АТС удобно производить в терминале хостовой машины, подключившись через SSH.

Для того, чтобы применить изменения, внесенные в конфигурационные файлы необходимо перезапустить Asterisk. Для этого в ОС OpenWRT используется команда

```
# /etc/init.d/asterisk restart
```

Также для перезапуска Asterisk можно просто перезагрузить виртуальную машину через интерфейс VirtualBox.

На АТС должна быть использована 5-значная нумерация, в которой первые две цифры обозначают индекс АТС, а оставшиеся цифры являются номером абонента. Двухзначные индексы АТС выбираются из табл. 3.4 согласно номеру учащегося в журнале группы.

Таблица 3.4

Индекс АТС.

Вариант выбирается по номеру учащегося в журнале группы

Вар.	Индекс	Вар.	Индекс	Вар.	Индекс	Вар.	Индекс	Вар.	Индекс
1	86	7	17	13	62	19	92	25	14
2	75	8	98	14	94	20	62	26	97
3	90	9	27	15	30	21	38	27	18
4	81	10	13	16	57	22	35	28	32
5	44	11	37	17	21	23	52	29	10
6	66	12	51	18	28	24	90	30	41

Программный клиент Linphone настраивается на хостовой ЭВМ. Программный клиент предустановлен и вызывается из главного меню ОС.

По окончании работы необходимо продемонстрировать преподавателю работоспособность построенной сети IP-телефонии, показав возможность осуществления звонка между абонентами АТС 1 и АТС 2.

План выполнения лабораторной работы

1. Сохранить и настроить виртуальную машину.
2. Настроить IP-АТС для выполнения локальных звонков.
3. Настроить совместную работу двух IP-АТС через IAX2-транк.

3.4. Контрольные вопросы

1. IP-АТС Asterisk.
2. Протокол SIP.
3. Протокол IAX2.

Лабораторная работа 4

Соединение узлов абонентского доступа через транзитный узел связи

4.1. Цель работы

Ознакомиться с принципами организации соединения узлов абонентского доступа через транзитный узел связи на примере системы IP-телефонии, разворачиваемой на базе программной IP-АТС Asterisk.

4.2. Теоретические сведения

4.2.1. Связь узлов доступа через транзитный узел связи

Согласно ГОСТ Р 53801-2010 под транзитным узлом связи (сети ПД) понимается узел связи, обеспечивающий транзит трафика между узлами связи.

В случае IP-АТС транзитный узел обеспечивает маршрутизацию вызовов абонентов, подключенных к узлам доступа. Использование транзитного узла связи упрощает обслуживание сети в случае большого числа узлов доступа, которые должны быть связаны между собой, позволяя перейти от топологии "каждый с каждым" к топологии "звезда" с транзитным узлом в центре.

Такой подход имеет ряд особенностей, которые необходимо учитывать при реализации. В частности:

1. В случае выхода транзитного узла из строя теряется возможность передачи данных между отдельными узлами доступа. Следовательно, необходимо обеспечить резервирование транзитного узла либо предусмотреть прямые маршруты передачи данных на наиболее нагруженных маршрутах между узлами доступа.

2. Транзитный узел должен обеспечить маршрутизацию всех соединений между абонентами разных узлов доступа. Следовательно, его аппаратное обеспечение и канал связи должны быть выбраны с учетом этого факта. Следует помнить, что транзитный узел должен обеспечивать работу сети в ЧНН. В случае значительного объема трафика между узлами доступа имеет смысл дублировать транзитный узел с целью балансировки нагрузки. Такое дублирование также решает и вопрос резервирования, обеспечивая "горячий резерв".

Рассмотрим пример сети с транзитным узлом на примере IP-АТС Asterisk. Такая схема может быть использована для связи отдельных филиалов распределенной компании между собой.

Пусть у нас есть два филиала, в которых установлены обслуживающие их IP-АТС **А** и **В**, соответственно. Они являются узлами доступа к услугам связи. Третья IP-АТС **Т** является транзитным узлом связи, обеспечивающим

маршрутизацию вызовов между абонентами узлов доступа **A** и **B**. Схема сети приведена на рис. 4.1.

На узлах доступа организована трехзначная нумерация абонентов, подключаемых по протоколу SIP. Узел доступа **A** имеет индекс 1. Узел доступа **B** имеет индекс 2. Таким образом, на сети доступа используется 4-значная нумерация абонентов. Узлы доступа **A** и **B** могут быть соединены с транзитным узлом связи **T** по протоколам IAX или SIP с использованием транковых каналов. На схеме на рис. 4.1 указан тип каналов SIP-trunk.

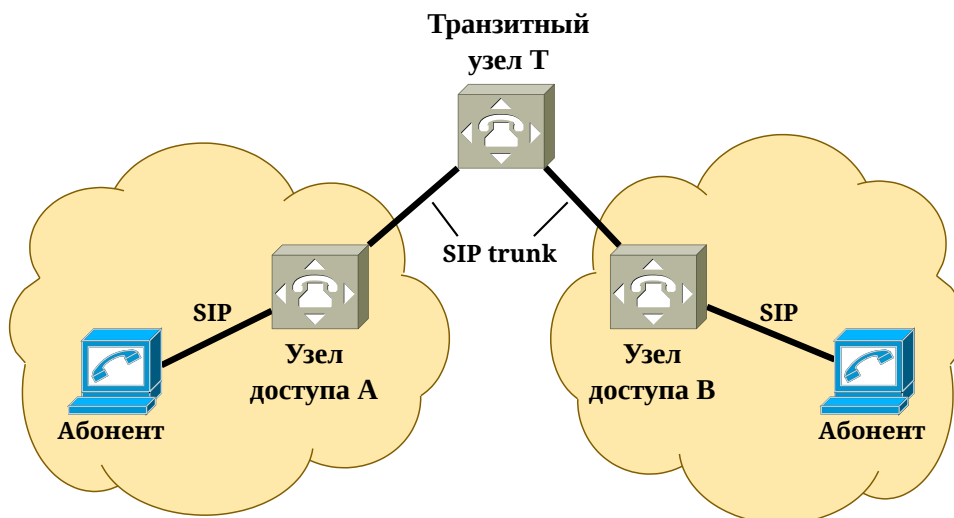


Рис. 4.1. Схема сети IP-телефонии. Связь узлов доступа через транзитную IP-АТС

4.2.2. Настройка IP-АТС Asterisk

4.2.2.1. Настройка абонентов узла доступа

При настройке учетных записей абонентов их часто прописывают в файлах `sip.conf`, `iax.conf` или других, соответствующих отдельным протоколам. Однако в Asterisk существует возможность настройки абонентов в отдельном специально предназначенном файле `users.conf`. Удобство этого способа в том, что он позволяет удобно настроить для одного пользователя различные методы доступа к услугам связи.

Для примера приведем простой конфигурационный файл `users.conf` для IP-АТС А, в котором заданы два абонента.

Листинг 4.1

Простой пример файла настройки `users.conf` для IP-АТС А

```
; Общие настройки для всех пользователей
; их можно переопределить для каждого пользователя в отдельности
[general]
fullname = New User
userbase = 001
; Активирует учетную запись SIP
```

```

hassip = yes
; Нижеследующие опции могут использоваться и в других файлах
; Они определяют дополнительные функции
; Уведомление абонента о входящем вызове при разговоре
callwaiting = yes
threewaycalling = yes
callwaitingcallerid = yes
transfer = yes
; Удержание вызова
canpark = yes
; Переадресация вызова
cancallforward = yes
; Звонки группам
callgroup = 1
pickupgroup = 1
; Контекст локального абонента (extensions.conf)
context = localsip
; Пользователь не привязан к конкретному адресу IP
host = dynamic

[1001]
callerid = Alice Smith (1001)
secret = 1234

[1002]
callerid = Bob Smith (1002)
secret = 1234

```

Следует обратить внимание на то, что лучше использовать в качестве номера абонента полный номер с учетом индекса. Это позволяет упростить настройку маршрутизации и обработки вызовов. Использование укороченных локальных номеров (3-значных в нашем примере) требует внесения дополнительных настроек для отображения корректных CallerID при входящем звонке.

4.2.2.2. Настройка SIP и SIP-trunk

SIP-trunk канал до транзитного узла удобно прописать в файле `sip.conf`, чтобы не смешивать его с обычными абонентами. В примере используется SIP-trunk с отдельной регистрацией, а привязка узла к IP-адресу реализована опциями `deny` и `permit`. Большинство опций описаны в предыдущей работе.

Листинг 4.2

Пример файла настройки sip.conf для IP-АТС А

```

[general]
allowguest=no
allowoverlap=no
alwaysauthreject=yes

```

```

useragent=OPDSPBX - A
sdpsession=OPDS PBX A
defaultexpire=3600
limitonpeer=yes
rtptimeout=360
rtpholdtimeout=300
rtpkeepalive=5
language=ru
bindport=5060
bindaddr=192.168.1.101
externip=192.168.1.101
localnet=192.168.1.0/255.255.255.0
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
nat=yes
dtmfmode=info
canreinvite=no
insecure=invite

; Регистрация узла А на транзитной станции
; Обратите внимание на необходимость использования адреса
; или доменного имени, а также на указание локальной записи pbxT
register => pbxA:passwA@192.168.1.100/pbxT

; Учетная запись для регистрации транзитной станции Т
; на узле А
[pbxT]
type=friend
transport=udp
context=from-trunk
; Для отдельной регистрации следующая опция обязательна
host=dynamic
; Задание адреса транзитного узла фильтром
deny=0.0.0.0/0.0.0.0
permit=192.168.1.100/32
; Пароль для подключения транзитного узла
secret=passwT

```

Аналогично настраивается узел **В**.

Далее приведем настройки транзитного узла **Т**.

Листинг 4.3

Пример файла настройки sip.conf для IP-АТС Т

```

allowguest=no
allowoverlap=no
alwaysauthreject=yes
useragent=OPDSPBX - T
sdpsession=OPDS PBX T

```



```
defaultexpire=3600
limitonpeer=yes
rtptimeout=360
rtpholdtimeout=300
rtpkeepalive=5
language=ru
bindport=5060
bindaddr=192.168.1.100
externip=192.168.1.100
localnet=192.168.1.0/255.255.255.0
srvlookup=yes
disallow=all
allow=alaw
allow=ulaw
nat=yes
dtmfmode=info
canreinvite=no
insecure=invite

; Регистрация транзитного узла на узлах доступа
register => pbxT:passwT@192.168.1.101/pbxA
register => pbxT:passwT@192.168.1.102/pbxB

; Общие настройки для учетных записей узлов доступа
[siptrunk](!)
type=friend
transport=udp
context=from-trunk
host=dynamic
deny=0.0.0.0/0.0.0.0

; Для отдельных узлов остается разрешить конкретный адрес
; и указать пароль
[pbxA](siptrunk)
permit=192.168.1.101/32
secret=passwA

[pbxB](siptrunk)
permit=192.168.1.102/32
secret=passwB
```

4.2.2.3. Настройка маршрутизации вызовов

Вначале рассмотрим маршрутизацию вызовов на узле доступа **А**. Маршрутизация на узле **В** реализуется аналогично.

Листинг 4.4

Пример файла маршрутизации вызовов extensions.conf для узла доступа А

```
[general]
static=yes
writeprotect=yes

[globals]

; В отличие от предыдущей работы здесь используется SIP-trunk,
; поэтому достаточно макроса для вызовов по SIP
[macro-dial-sip]
exten => s,1,NoOp()
exten => s,n,Dial(SIP/${ARG1},20,tT)
exten => _s-.,n,Hangup()

[default]

[incoming_calls]

; Контексты локальных пользователей
; Обратите внимание на то, что вначале идет обработка местных звонков,
; а затем обработка исходящих звонков. Это позволяет не фильтровать
; индекс в контексте исходящих вызовов [remote]
[localsip]
include => internal
include => remote

; Поскольку пользователей задаем полным номером,
; при звонке по укороченному номеру перед ним надо добавить индекс
; В нашем примере это 1
[internal]
exten => _XXX,1,Macro(dial-sip,1${EXTEN})
exten => _1XXX,1,Macro(dial-sip,${EXTEN})

; Все вызовы на четырехзначные номера отправлять на транзитный узел
; Фильтрация местных номеров обеспечивается порядком обработки записей
; в контексте локальных пользователей [localsip]
[remote]
exten => _XXXX,1,Macro(dial-sip,pbxT/${EXTEN})

; Входящие вызовы из транка могут обратиться только к локальным номерам
[from-trunk]
include => internal
```

Теперь приведем пример маршрутизации на транзитном узле **T**. На нем нет местных абонентов, поэтому обрабатываются только вызовы из транковых каналов, которые переадресуются на соответствующие узлы доступа согласно индексам.

Листинг 4.5

Пример файла маршрутизации вызовов extensions.conf для транзитного узла T

```
[general]
static=yes
writeprotect=yes

[globals]

[macro-dial-sip]
exten => s,1,NoOp()
exten => s,n,Dial(SIP/${ARG1},20,tT)
exten => _s-.,n,Hangup()

[default]

[incoming_calls]

[from-trunk]
exten => _1XXX,1,Macro(dial-sip,pbxA/${EXTEN})
exten => _2XXX,1,Macro(dial-sip,pbxB/${EXTEN})
```

4.2.3. Список использованных источников

1. Asterisk // Материал с сайта Wikipedia.org. URL: <https://ru.wikipedia.org/wiki/Asterisk>.
2. IAX // Материал с сайта Voip-info.org. URL: <https://www.voip-info.org/iax/>.
3. Asterisk SIP NAT solutions // Материал с сайта Voip-info.org. URL: <https://www.voip-info.org/asterisk-sip-nat-solutions/>.
4. Linphone open-source voip software // Материал с сайта Linphone.org. URL: <http://www.linphone.org/>.
5. Linphone // Материал с сайта Wikipedia.org. URL: <https://ru.wikipedia.org/wiki/Linphone>.

4.3. Порядок выполнения лабораторной работы

Лабораторная работа предназначена для выполнения двумя бригадами студентов не более двух человек каждая. Допускается выполнение на личных ноутбуках, в том случае, если обе бригады используют личные ноутбуки и эти ноутбуки способны запускать виртуальные машины.

По результатам работы должен быть сделан отчет. По каждому пункту должны быть указаны: команда и результат выполнения команды (в текстовом формате). По каждому подразделу должны быть сделаны и написаны выводы. Отчет должен быть оформлен в электронном виде в формате PDF и выслан на электронную почту преподавателя. Допускается также сдача печатного экземпляра отчета (в этом случае листы отчета не должны быть сшиты, допускается только скрепление листов на канцелярскую скрепку).

В работе необходимо реализовать связь двух узлов доступа (АТС 1 и АТС 2) через транзитный узел с помощью каналов SIP-trunk, аналогично тому, как это показано в примере. Способ описания пользователей (users.conf или sip.conf) на усмотрение учащихся.

На АТС должна быть использована 5-значная нумерация, в которой первые две цифры обозначают индекс АТС, а оставшиеся цифры являются номером абонента. Двухзначные индексы АТС выбираются из табл. 4.1 согласно номеру учащегося в журнале группы.

Таблица 4.1

Индекс АТС.

Вариант выбирается по номеру учащегося в журнале группы

Вар.	Индекс	Вар.	Индекс	Вар.	Индекс	Вар.	Индекс	Вар.	Индекс
1	86	7	17	13	62	19	92	25	14
2	75	8	98	14	94	20	62	26	97
3	90	9	27	15	30	21	38	27	18
4	81	10	13	16	57	22	35	28	32
5	44	11	37	17	21	23	52	29	10
6	66	12	51	18	28	24	90	30	41

Программный клиент Linphone настраивается на хостовой ЭВМ. Программный клиент предустановлен и вызывается из главного меню ОС.

По окончании работы необходимо продемонстрировать преподавателю работоспособность построенной сети IP-телефонии, показав возможность осуществления звонка между абонентами АТС 1 и АТС 2.

План выполнения лабораторной работы

1. Сохранить и настроить виртуальную машину (см. предыдущую лабораторную работу).
2. Настроить IP-АТС для выполнения локальных звонков.
3. Настроить транзитную IP-АТС.
4. Настроить совместную работу двух АТС 1 и АТС 2 через транзитную АТС с использованием каналов SIP-trunk.

4.4. Контрольные вопросы

1. IP-АТС Asterisk.
2. Протокол SIP.
3. Протокол IAX2.

Владимиров Сергей Сергеевич

**ТЕХНОЛОГИИ АБОНЕНТСКОГО ДОСТУПА В РАСПРЕДЕЛЕННЫХ
СПД**

Лабораторный практикум

Редактор *Х. Х. Хxxxxxxxxx*

План изданий 20XX г., п. XX

Подписано к печати XX.XX.20XX
Объем X,XX усл.-печ. л. Тираж XX экз. Заказ XXX

Редакционно-издательский отдел СПбГУТ
193232 СПб., пр. Большевиков, 22
Отпечатано в СПбГУТ