

Лабораторная работа № 3. Настройка исходящей маршрутизации вызовов и опций безопасности на IP-АТС.

Цель работы: осуществить сопряжение IP-АТС с вышестоящим провайдером услуг, выполнить настройку дополнительных опций безопасности IP-АТС.

Задание:

Запустить IP-АТС и подключиться к консоли управления для настройки АТС;

Зарегистрировать учетную запись у вышестоящего провайдера и подключить IP-АТС к провайдеру;

Настроить исходящую маршрутизацию и проверить работоспособность;

Настроить функционал ограничения допустимого IP-адреса VoIP-терминала пользователя;

Схема лабораторной установки

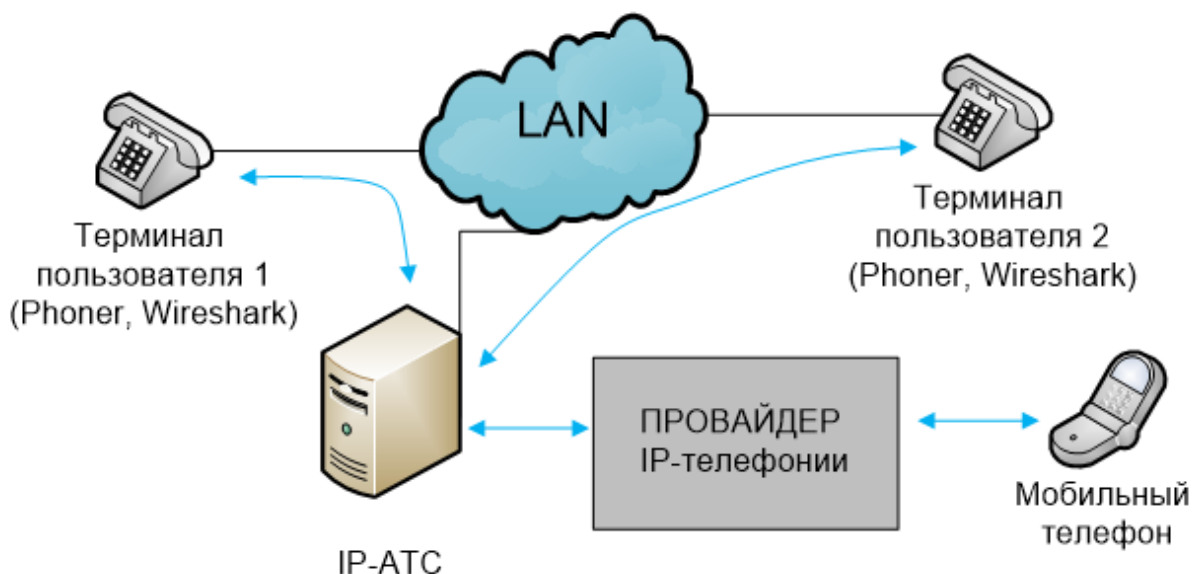


Рисунок 3.1 – Схема лабораторной установки

Руководство:

Все студенты делятся на несколько бригад. Каждой бригаде необходимо два компьютера с установленными программным клиентом IP-телефонии Phoner и сетевым анализатором Wireshark. Один из компьютеров также используется, как IP-АТС.

Часть 1– Настройка разрешенного IP-адреса для VoIP-терминала пользователя.

1. Запустить IP-АТС, установленную в предыдущей лабораторной работе.

2. Зайти через веб-браузер на интерфейс управления IP АТС
3. Создать четвертого SIP-пользователя на IP-АТС с телефонным номером 10G4, где G - порядковый номер бригады студентов.
4. Настроить разрешенные IP-адреса для SIP-пользователей 3 и 4.
5. Определить текущие IP-адреса SIP-пользователей 3 и 4. В командной строке на терминале SIP-пользователя ввести команду ipconfig.

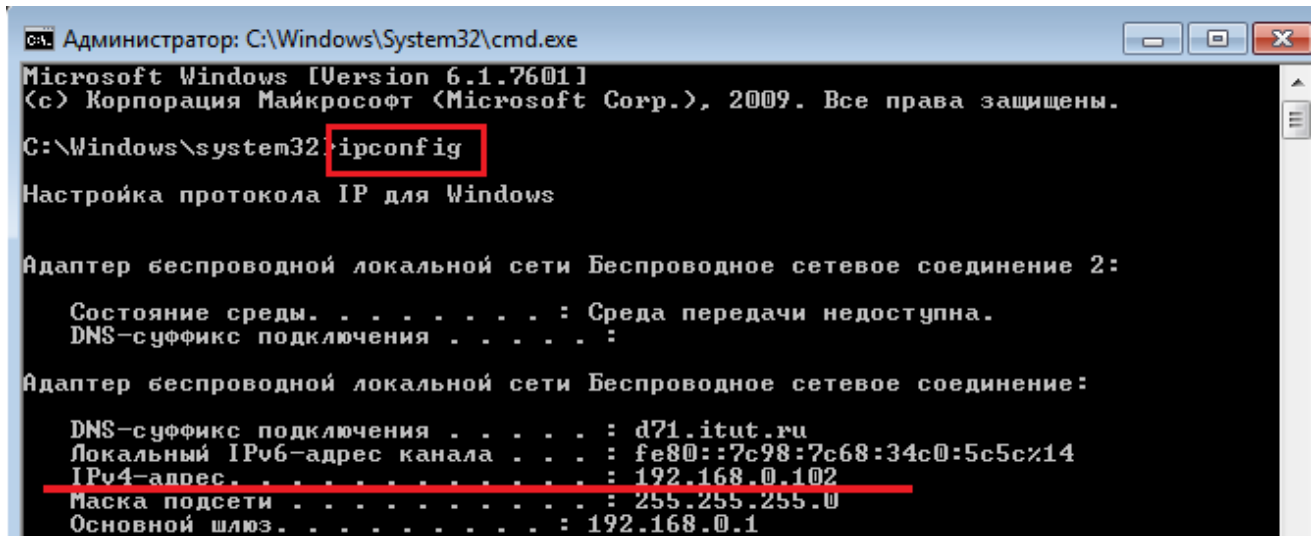


Рисунок 3.2– Проверка IP-адреса SIP-пользователя

6. Далее в настройках IP-АТС во вкладке "PBX\PBX Configuration\Extensions" выбрать один из добавленных extension, соответствующий SIP-пользователю 3. В строке permit указать IP-адрес SIP-пользователя 3. Обратите внимание, что для настройки в качестве разрешенного только одного IP-адреса, в строке permit указывается маска 255.255.255.255. Маска 255.255.255.0 – это маска всей подсети пользователя. Пример настроек приведен на рисунке 3.3.

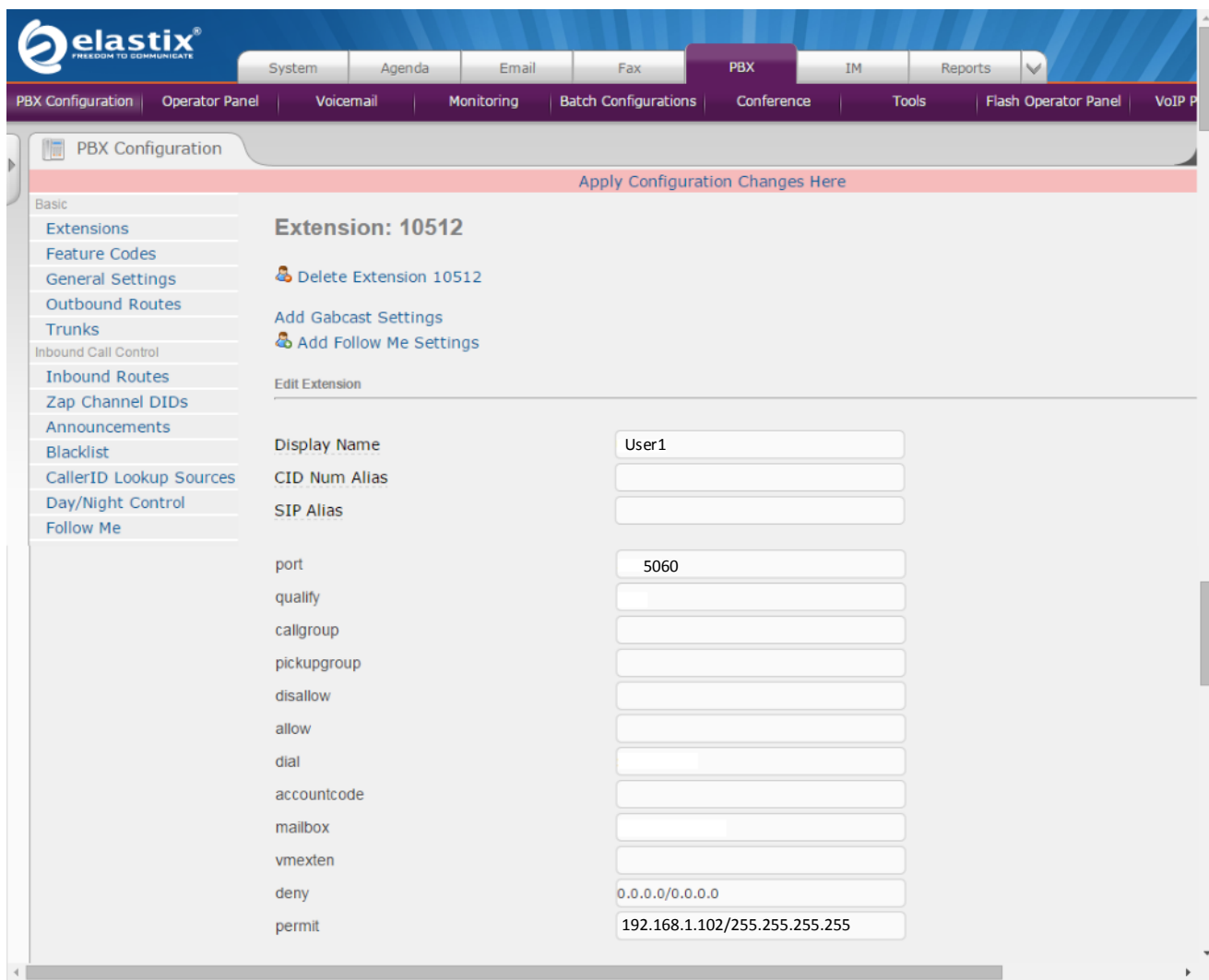


Рисунок 3.3– Пример настройки разрешенного IP-адреса

Далее, необходимо нажать кнопку «Submit» и нажать на красную полосу "Apply configuration changes here".

7. Чтобы проверить успешность регистрации терминалов пользователя 3 и терминалов пользователя 4, в браузере перейти во вкладку "PBX/PBX configuration". В нижней части меню необходимо выбрать пункт «Unembedded free PBX».

В случае отсутствия доступа к вкладке «Unembedded free PBX» - перейти во вкладку «Security – Advanced settings», как показано на рисунке 3.4, и установить переключатели на ON, а также ввести пароль.

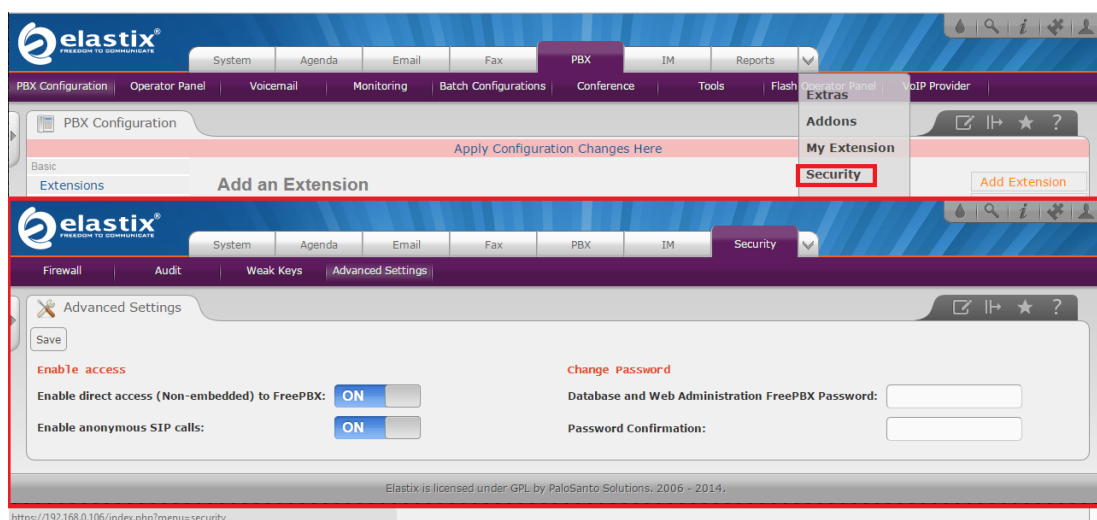


Рисунок 3.4– Активация доступа к модулю «Unembedded free PBX»

В появившемся окне, представленном на рисунке 3.5, выбрать "Tools/AsteriskInfo/Registries". В таблице будут указаны все зарегистрированные пользователи. Пример вывода приведен на рисунке 3.6.

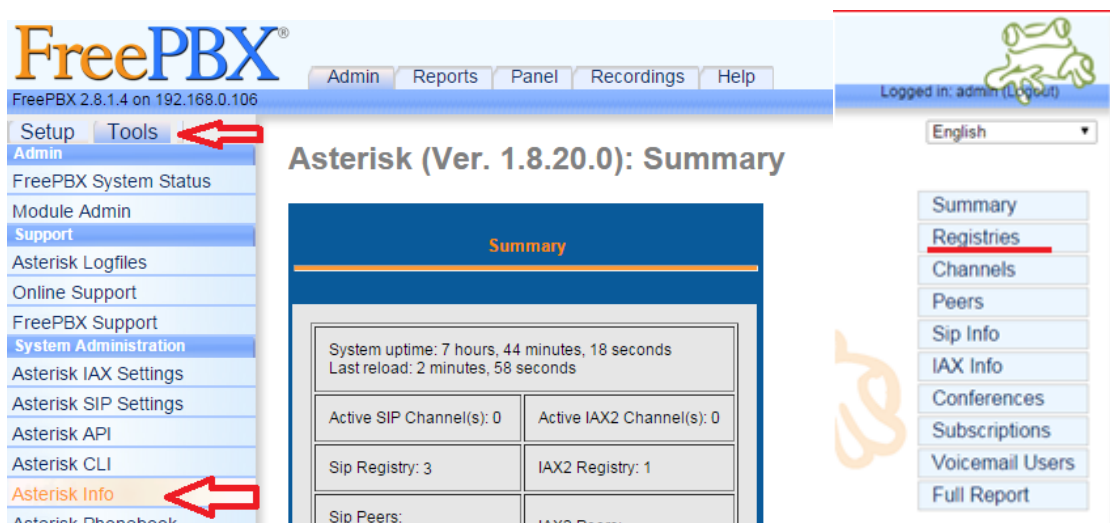


Рисунок 3.5–Модуль «Unembedded free PBX»

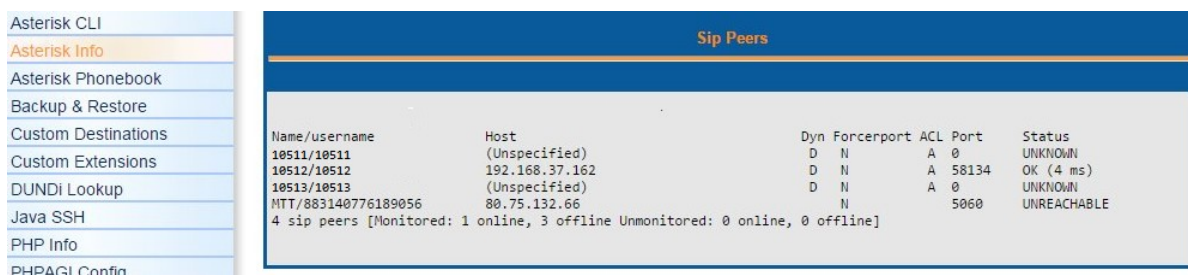


Рисунок 3.6 – Отображение зарегистрированных пользователей в модуле «Unembedded free PBX»

- Создать дампы регистрации SIP-пользователя 4 и дампы звонка от SIP-пользователя 3 к SIP-пользователю 4.

9. Вместо SIP-пользователя 4 можно выполнить соединение с терминала 3 на один из служебных номеров: эхо тест (*43), номер абонента (*65) или говорящие часы Speaking Clock(*60). Проверить, что звонок проходит. Сделать скриншот обмена SIP-сообщениями во время звонка. Сохранить дампы для дальнейшего анализа.
10. Для SIP-пользователя 3 поменять значение IP-адреса в строке permit на 8.8.8.8/255.255.0.0. Для этого во вкладке "PBX\PBX configuration\Extensions" выбрать Extension, соответствующий SIP-пользователю 3. В поле permit поменять значение на 8.8.8.8/255.255.0.0, как показано на рисунке 3.7.

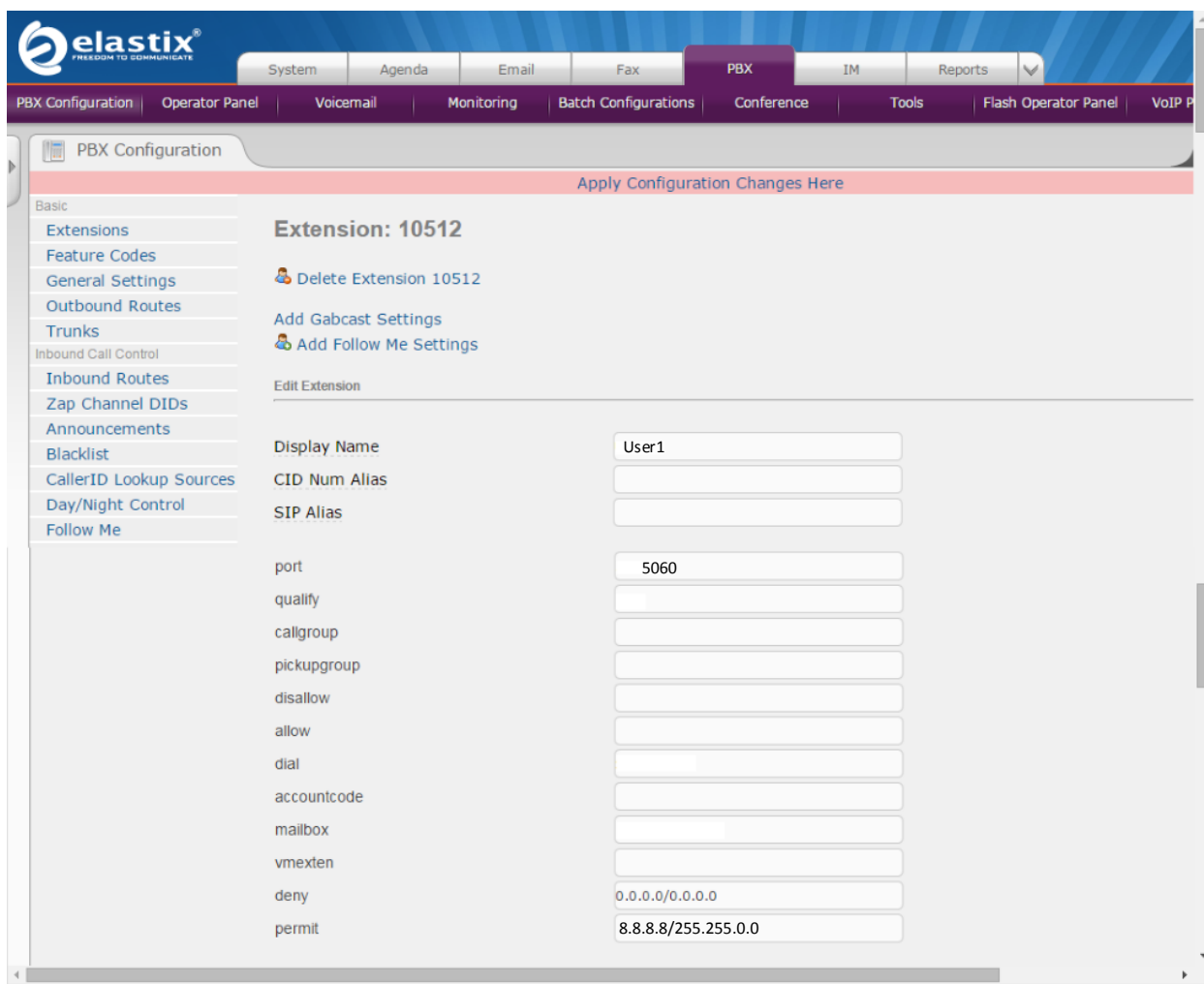


Рисунок 3.7 –Изменение разрешенного IP-адреса

11. Проверить возможность регистрации пользователя 3 после установки некорректного IP-адреса в поле permit. Теперь необходимо запустить повторно дампы в Wireshark, попробовать с помощью Phoner позвонить с терминала SIP-пользователя 3 на терминал SIP-пользователя 4. В случае правильных настроек SIP-пользователь 3 не сможет регистрироваться на IP-АТС. Звонок проходить также не будет, так как фактический IP-адрес

SIP-пользователя 3, и разрешенный IP-адрес, указанный в поле permit, будут отличаться.

Необходимо сохранить полученный дамп в Wireshark, сделать скриншот обмена SIP-сообщениями, выполнить анализ дампа и подготовить SIP Flow.

Часть 2–Установка исходящей маршрутизации

1. Зарегистрируйтесь на сайте VoIP оператора для получения авторизационных данных для подключения IP-АТС к вышестоящей сети. Далее приведена регистрация на примере Your Magic. Для получения персонального аккаунта для настроек SIP необходимо перейти на сайт <http://www.youmagic.com/> и пройти процедуру регистрации. При регистрации выбрать пункт - Международный номер (номер должен начинаться с 88314). После регистрации на сайте вам придет письмо на указанный адрес электронной почты. Необходимо активировать свой аккаунт, перейдя по ссылке в письме, и запомнить свой логин и пароль для дальнейшей настройки АТС.
2. Необходимо запустить Phoner или любой другой VoIP клиент для регистрации с использованием своего аккаунта и проверить, что он работает и что ACL пропускают SIP-соединение.
3. Настройка SIP-trunk на IP-АТС. Для этого в браузере перейти во вкладку "PBX/PBX Configuration/Trunks" и выбрать SIP trunk, выполнить настройку согласно примеру, приведенному на рисунке 3.9.

При настройке необходимо указать шаблон для исходящих номеров, звонки на которые могут передаваться через настраиваемый SIP trunk. Представленный на примере шаблон позволяет звонить на мобильные номера, имеющие префикс "8" и длину 11 цифр, где остальные 10 цифр принимают значения от 0 до 9 (чему соответствует X в шаблоне).

Add SIP Trunk

General Settings

Trunk Name:

Outbound Caller ID:


CID Options:

Maximum Channels:

Disable Trunk: ☐ Disable

Monitor Trunk Failures: ☐ Enable

Dialed Number Manipulation Rules

(| 

Dial Rules Wizards:

Outbound Dial Prefix:

Outgoing Settings

Trunk Name:

PEER Details:

```
username=1111
type=friend
secret=UserPASS
qualify=yes           fromuser=1111
port=5060
nat=yes
insecure=port,invite
host=voip.mtt.ru
fromuser=1111
fromdomain=voip.mtt.ru
dtmfmode=rfc2833
disallow=all
allow=alaw
```

Incoming Settings

USER Context:

USER Details:

```
type=user
secret=UserPASS
context=from-trunk
```

Registration

Register String:

Рисунок 3.9 - Пример настройки SIP-trunk

После выполнения настроек нажать кнопку "Submit changes" и на красную полосу "Apply changes". Пример настроек также представлен в таблице 3.1.

Таблица 3.1. Пример настроек для SIP-trunk.

PEER Details: username=UserPHONE type=friend secret=UserPASSWORD qualify=yes port=5060 nat=yes insecure=port,invite host=voip.mtt.ru fromuser=UserPHONE fromdomain=voip.mtt.ru dtmfmode=rfc2833 disallow=all allow=alaw	USER Details: type=user secret=UserPASSWORD context=from-trunk Register String: UserPHONE:UserPASSWORD@voip.mtt.ru:5060/UserPHONE
---	---

Ниже представлены пояснения к примеру настроек из таблицы 3.1.

Формат регистрации: user [:secret] @host [:port] [/extension]

User – идентификатор пользователя, используемый для SIP сервера (например, 2345).

Secret – пароль пользователя.

Host – имя домена или хоста SIP сервера.

Port – на какой номер UDP/TCP порта посылать запросы на регистрацию на сервере host. По умолчанию - 5060

/1234 – номер пользователя для приема вызовов.

Тип SIP клиента может быть: "user", "peer" или "friend".

nat - эта переменная изменяет образ действия сервера Asterisk для клиентов, находящихся за межсетевым экраном с трансляцией адресов (NAT). Но этот параметр не решает проблемы, если сам Asterisk находится за таким межсетевым экраном, а клиент снаружи, в сети Internet с публичным IP адресом.

allow=<codec>: разрешенные кодеки, порядок выбора кодека, задается порядком их описания в этой команде (Сначала используйте: DISALLOW=ALL, перед тем, как разрешить какие-то конкретные кодеки)
 dtmfmode: inband | info | rfc2833 (глобальная настройка).
 fromdomain=<domain>: установка домена по умолчанию.
 port: SIP порт клиента.
 qualify: периодическая проверка доступности клиента.
 fromuser: указывается имя пользователя для поля "from", когда происходит вызов с использованием этой записи
 host: IP адрес или имя хоста сервера.
 insecure: very|yes|no|invite|port: определяет, как обрабатывать соединения с пирами.

4. Включить поддержку NAT в IP-АТС. Для включения опции NAT в браузере нужно открыть вкладку "PBX/Unembedded free PBX/Tools/Asterisk SIP Settings" и установить значения, как показано на рисунке 3.10: Nat – Yes, IP Configuration– Static.

Сделать скриншот выполненных настроек.

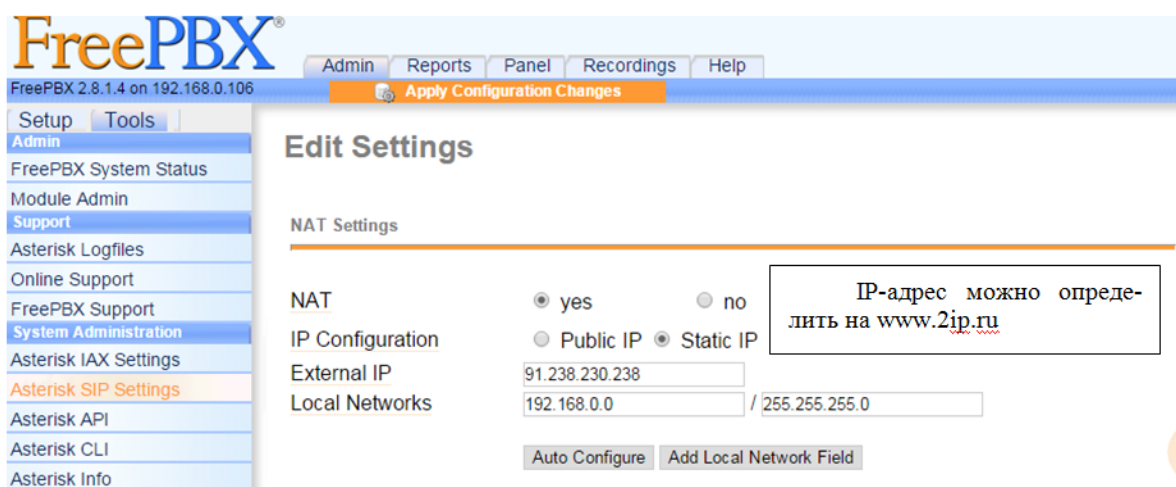
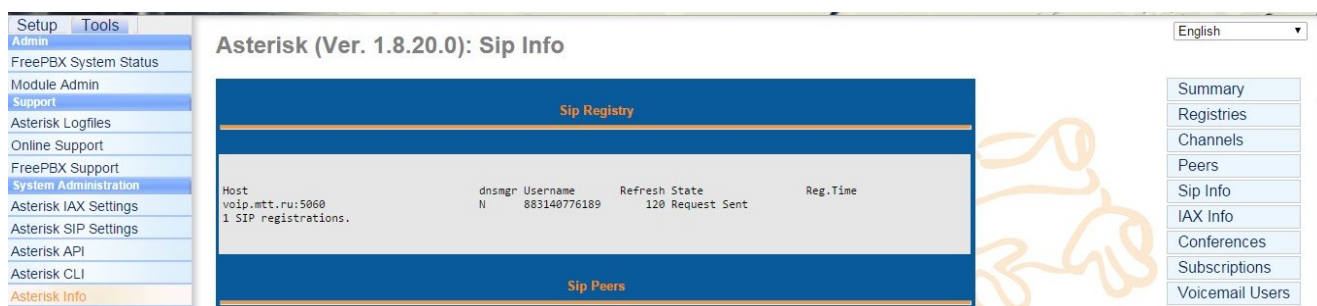


Рисунок 3.10 – Пример настройки NAT

5. Проверка регистрации IP-АТС на сервере оператора. Для этого зайти во вкладку "PBX/Unembedded free PBX/Tools/Asterisk Info/Registries", как показано на рисунке 3.11.



6. Сделать скриншот страницы.

7. Настройте маршрутизации для исходящих звонков и digit manipulation.

Для настройки маршрутизации необходимо настроить шаблоны (паттерны) для исходящих номеров, которые пользователи IP-телефонии будут набирать, а также указать SIP-trunk, который будет применяться при исходящих звонках. Для настройки необходимо перейти в меню настройки Outbound Routes во вкладку PBX/PBX configuration/Outbound Routes.

Данный модуль управляет исходящей маршрутизацией во FreePBX. На основании набранного номера выбирается направление (транк) для исходящего вызова. Набираемый номер делится на префикс и паттерн и может модифицироваться после набора. Пример настроек приведен на рисунке 3.12.

Программа Phoner при совершении звонка может подставлять в начало номера цифру 0. Для этого в паттерне используется digit manipulation– вырезание первой цифры номера "0", как показано в примере на рисунке 3.12. Если используется другое программное обеспечение для совершения звонка (например, Zoiper), то вырезание 0 не требуется и в паттерне из примера необходимо удалить префикс 0. Заполнение выполняется согласно рекомендациям:

Route Name –описательное название маршрута;

Route CID– настройка замены CallerID абонента на указанное значение;

Route Password –настройка пароля на маршрут. Если установлено значение - при звонке через это направление будет предложено ввести пароль. При вводе неправильно пароля - соединение будет разорвано.

Dial Patterns –настройка шаблонов, при наборе которых будет использовано направление. Выполняется в соответствии с правилами заполнения шаблона:

X – цифры 0 - 9

Z – цифры 1 - 9

N – цифры 2 - 9

[1237-9] – любая цифра или буква в скобках (в примере 1,2,3,7,8,9)

. - точка – любой знак.

Пример: Абонент набирает 8. 8 удаляется и подставляется +7. Точка символизирует любую последовательность цифр. Таким образом, делаются возможные звонки на номер мобильного телефона. Также можно использовать более простой шаблон, где указывается только префикс 8, а в соответствии остальным 10-ти цифрам указываются XXXXXXXXXXXX. Пример приведен на рисунке 3.13.

Route Settings

Route Name:

Route1

Route CID:

1

☒ Override Extension

Route Password:

Route Type:

☐ Emergency ☐ Intra-Company

Music On Hold?

default

Time Group:

---Permanent Route---

Route Position

---No Change---

Additional Settings

PIN Set:

None

Dial Patterns that will use this Route

(prepend)

+

8XXXXXX

/

CallerId

(prepend)

+

prefix

|

[match pattern

/

CallerId

+ Add More Dial Pattern Fields

Dial patterns wizards:

(pick one)

Trunk Sequence for Matched Routes

0

trunktoprovider

1

Add Trunk

Submit Changes

Рисунок 3.12 – Пример настройки паттерна.

Dial Patterns that will use this Route

(+7) + 8 | [. / CallerId]

Рисунок 3.13. Пример настройки шаблона.

8. Проверка выполненных настроек. Попробуйте позвонить с SIP-терминала пользователя на мобильный телефон или на другой телефон из ТфОП. Сделайте дамп звонка. Если соединение с внешним абонентом проходит успешно – настройки выполнены корректно.
9. Сохраните дамп для последующего анализа.

Отчет

Отчет должен содержать наименование работы, цели и задачи, скриншоты по каждому пункту заданий и комментарии, а также выводы.

Проверка выполнения работы

Вы выполнили работу, если

1. Созданный SIP-пользователь 3 успешно зарегистрировался на IP-АТС и может совершать вызовы 1 и 2 пользователя.
2. При звонке с терминала SIP-пользователя 1 на терминала SIP-пользователя 2 соединение проходит успешно при соответствии реального IP-адреса пользователя и адреса, настроенного в поле permit.
3. При звонке с терминала SIP-пользователя 1 на терминала SIP-пользователя 2 соединение не проходит успешно при несоответствии реального IP-адреса пользователя и адреса, настроенного в поле permit.
4. IP-АТС успешно прошла регистрацию на сервере оператора
5. Успешно работает исходящая маршрутизация и вы можете выполнить звонок на свой мобильный телефон с терминала пользователя.

Вопросы для подготовки:

- Как создается аккаунт SIP-пользователя на IP-АТС?
- Для чего используются опции permit / deny в профиле SIP-пользователя?
- Какие основные настройки выполняются на АТС при подключении к оператору IP-телефонии?
- Каково основное назначение SIP-транк для АТС?
- Как настраивается SIP-транк на АТС?
- Как используется digit manipulation при настройке исходящей маршрутизации.
- Как настраивается маршрутизация вызовов на АТС?

