

IT база знаний
wiki.merionet.ru

Бесплатный курс по Asterisk

УСТАНОВКА, НАСТРОЙКА, БЕЗОПАСНОСТЬ, ТРАБЛШУТИНГ



МЕРИОН НЕТВОРКС

Блок 5.

Траблшутинг Asterisk

Обзор

1. [Как снять логи с Asterisk с помощью FreePBX?](#)
2. [Время хранения логов в Asterisk](#)
3. [Обзор модуля Asterisk Log](#)
4. [Проблемы со слышимостью в Asterisk](#)
5. [Sngrep: установка и использование](#)
6. [Домашнее задание.](#)

Как снять логи с Asterisk с помощью FreePBX?

От проблем и неполадок не застраховано ничто и **IP-АТС Asterisk** – не исключение. Неправильная конфигурация, неудачное обновление, неполадки в сети, сбой у провайдера - всё это может тем или иным образом сказываться на работе Вашей системы IP-телефонии. Для того, чтобы решить эти проблемы или хотя бы найти правильный путь, в сторону которого следует “копать”, нужно собственно, услышать показания “пациента”, то есть – нашего сервера IP-АТС Asterisk. Говоря простым языком – нужно снять логи. А с помощью модуля FreePBX, о котором мы хотим рассказать в данном разделе, сделать это будет еще проще.

Итак, для того чтобы решить проблему нам нужна информация. Но слишком большое количество информации может быть так же бесполезно, как и её отсутствие. В разделе мы покажем, как собрать полезную и краткую информацию.

Где Asterisk хранит логи?

Чтобы знать что “**лечить**”, нужно знать где искать. Информация, которую мы ищем содержится во множестве лог-файлов, которые хранит сервер.

Важно! Обратите внимание, что в зависимости от используемого дистрибутива Linux, расположение лог-файлов у Вас может быть другим.

| Расположение | Описание |
|--|--|
| /var/log/asterisk/fail2ban | Журнал событий модуля fail2ban |
| /var/log/asterisk/freepbx.log | Журнал событий модулей FreePBX |
| /var/log/asterisk/freepbx_security.log | Журнал событий безопасности |
| /var/log/asterisk/full | Журнал событий Asterisk каждого уровня. Обычно используется для поиска трассировок старых звонков |
| /var/log/dmesg | Журнал событий уровня ядра |
| /var/log/httpd/access_log | Журнал событий доступа к Apache |
| /var/log/httpd/error_log | Журнал ошибок web сервера Apache |
| /var/log/messages | Системный журнал событий Linux |
| /var/log/yum.log | Журнал действий, выполненных через yum |

Названия файлов могут быть дополнены информацией о дате, за которую создан файл, указанную после (.) или (-)

Фильтрация

Некоторые из этих файлов могут содержать тысячи записей, поэтому, если Вы знаете, какое событие ищете, то отфильтруйте лог по данному событию или хотя бы сократите его, например, оставьте только информацию за определённое время.

Чтобы найти нужную информацию, используйте утилиту `grep`, которая позволяет искать определённые шаблоны или части слов в большом количестве записей.

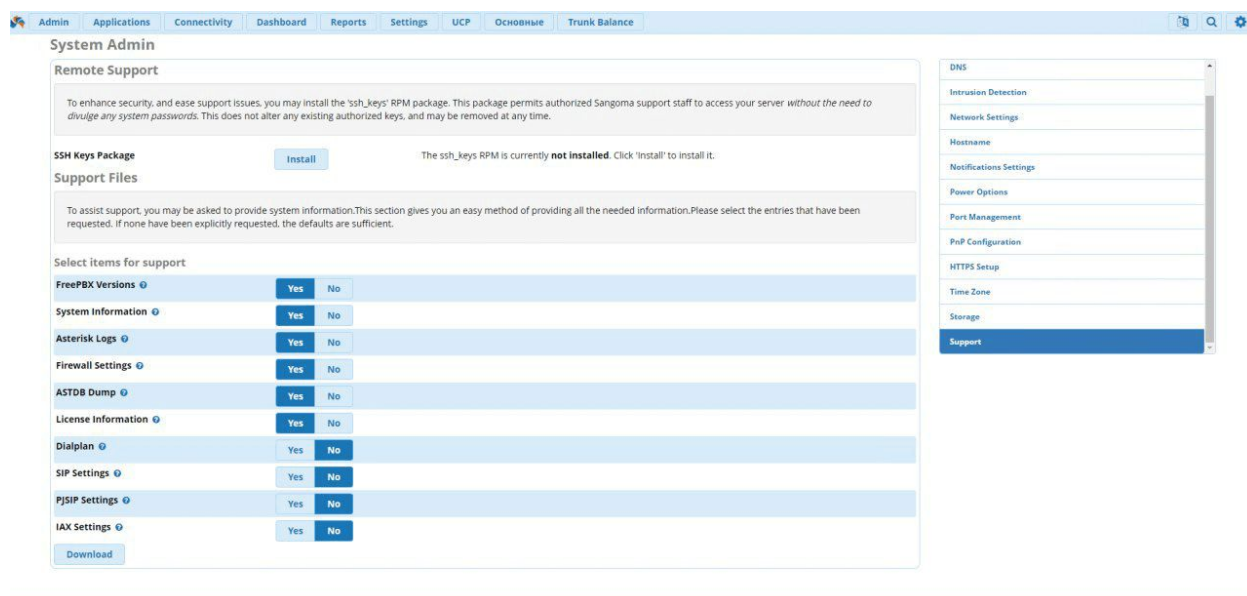
```
grep 10987 /var/log/asterisk/full
```

В примере выше мы ищем совпадение записей по числам **10987** в полном журнале событий Asterisk

Если Вы хотите попросить помощи на общедоступных площадках, например, на форуме, то рекомендуем удалить или изменить всю приватную/ секретную информацию, которую может содержать лог, такую как номера телефонов, публичные IP-адреса, ваш account ID у провайдера, пароли и т.д.

Модуль Support FreePBX

В версии 13 и 14 FreePBX, в модуле System Admin есть очень полезная секция - **Support**. Для того, чтобы попасть в неё необходимо перейти по следующему пути из дашборда кликнуть на вкладку **Admin → System Admin → Support**, перед Вами откроются доступные опции данной секции:



На этой странице, Вы можете скачать ZIP – файл, который будет содержать отчёт с необходимой системной информацией и логи для дальнейшего исследования или же для отправки в техническую поддержку.

Для включения информации в отчет используйте кнопки **Yes/No**. Рассмотрим каждый пункт, который можно включить в отчет:

- **FreePBX Versions** - Список всех установленных модулей и их версии
- **System Information** - Информация об операционной системе
- **Asterisk Logs** - Журналы событий Asterisk за последние 24 часа
- **Firewall Setting** - Вывод текущих настроек ip-tables
- **ASTDB Dump** - Полный дамп ASTBD (Не путать с MySQL)
- **License Information** - Информация о лицензировании и статусе сервера
- **Dialplan** - Полный дайл-план, созданный FreePBX (включая кастомные файлы _custom)
- **SIP Settings** - Настройки SIP (Может содержать секретную информацию)

- **PJSIP Settings** - Настройки PJSIP (Может содержать секретную информацию)
- **IAX Settings** - Настройки IAX (Может содержать секретную информацию)

Как только Вы выбрали какую информацию хотите включить в отчет, нажмите кнопку **Download** и сохраните ZIP файл на свой компьютер.

На этой странице, Вы также можете установить ssh, ключи, которые позволят сотрудникам технической поддержки Sangoma подключиться к Вашей системе без необходимости разглашать всякие пароли.

Время хранения логов в Asterisk

По умолчанию, в дистрибутиве FreePBX Distro большинство лог – файлов Asterisk сконфигурированы на хранение в течение семи дней. Зачастую, пользователи жалуются на технические проблемы (недозвон, короткие гудки, обрыв и так далее) спустя недели, а порой и месяцы. Именно по этой причине, в разделе расскажем как настроить хранение лог – файлов на более длительное время и как добавить сжатие для них, чтобы сохранить место на жестких дисках.

Настройка

За длительность хранения отвечает файл `/etc/logrotate.d/asterisk`. Давайте откроем его редактором **vim** и увеличим время хранения по нужным файлам до 45 дней:

```
[root@asterisk ~]# vim /etc/logrotate.d/asterisk
```

И для файла `/var/log/asterisk/freepbx_dbug` меняем параметр `rotate` с 7 на 45:

```
/var/log/asterisk/freepbx_dbug{
    daily
    missingok
    rotate 45 //меняем данное значение для
увеличения времени хранения в днях;
    notifempty
    compress //добавляем параметр compress, для
активации сжатия;
    sharedscripts
    create 0640 asterisk asterisk
}
```

Важно: С увеличением времени хранения файлов, увеличивается и его объем, занимаемый на жестких дисках сервера. При добавлении параметра `compress` в конфигурационную секцию, файл будет сжиматься с помощью утилиты компрессии **gzip**

Как можно увидеть в нашем примере, для лог – файла `/var/log/asterisk/freepbx_dbug` выставлен параметр **daily** (ежедневно), который регламентирует значение параметра **rotate**. Это означает, что значение 45 будет интерпретировано днями. Если вы хотите указывать значение параметра `rotate` в месяцах, то укажите здесь вместо **daily** **monthly** (ежемесячно).

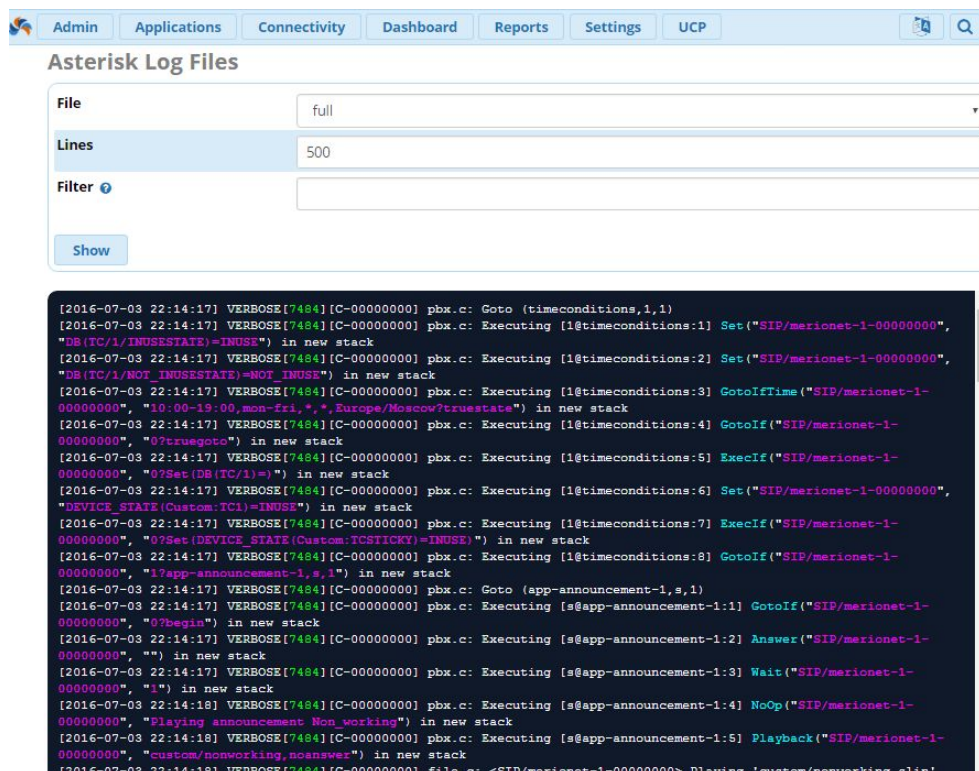
По завершению настроек сохраните их нажатием **:x! + Enter** - изменения вступят в силу.

Обзор модуля Asterisk Log

Существует встроенный модуль для **FreePBX - Asterisk Logfiles Module**, который позволяет просмотреть самые недавние события.

Смотрит логи с помощью FreePBX

Модуль можно найти по следующему пути: **Reports – Asterisk Logfiles**.



The screenshot displays the 'Asterisk Log Files' interface within the FreePBX web application. The top navigation bar includes 'Admin', 'Applications', 'Connectivity', 'Dashboard', 'Reports' (which is active), 'Settings', and 'UCP'. Below the navigation bar, the 'Asterisk Log Files' section contains a form with a 'File' dropdown menu set to 'full', a 'Lines' input field set to '500', and a 'Filter' input field. A 'Show' button is located below the form. The log output is displayed in a dark-themed text area, showing various Asterisk log messages with timestamps and details about call processing, including conditions, stack frames, and announcements.

```
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Goto (timeconditions,1,1)
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:1] Set("SIP/merionet-1-00000000",
"DB(TC/1/INUSESTATE)=INUSE") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:2] Set("SIP/merionet-1-00000000",
"DB(TC/1/NOT_INUSESTATE)=NOT_INUSE") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:3] GotoIfTime("SIP/merionet-1-
00000000", "10:00-19:00,mon-fri,*.*,Europe/Moscow?truestate") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:4] GotoIf("SIP/merionet-1-
00000000", "0?truegoto") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:5] ExecIf("SIP/merionet-1-
00000000", "0?Set(DB(TC/1)=)") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:6] Set("SIP/merionet-1-00000000",
"DEVICE_STATE(Custom:TC1)=INUSE") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:7] ExecIf("SIP/merionet-1-
00000000", "0?Set(DEVICE_STATE(Custom:TCSTICKY)=INUSE)") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [1@timeconditions:8] GotoIf("SIP/merionet-1-
00000000", "1?app-announcement-1,s,1") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Goto (app-announcement-1,s,1)
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [s@app-announcement-1:1] GotoIf("SIP/merionet-1-
00000000", "0?begin") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [s@app-announcement-1:2] Answer("SIP/merionet-1-
00000000", "") in new stack
[2016-07-03 22:14:17] VERBOSE[7484][C-00000000] pbx.c: Executing [s@app-announcement-1:3] Wait("SIP/merionet-1-
00000000", "") in new stack
[2016-07-03 22:14:18] VERBOSE[7484][C-00000000] pbx.c: Executing [s@app-announcement-1:4] NoOp("SIP/merionet-1-
00000000", "Playing announcement Non_working") in new stack
[2016-07-03 22:14:18] VERBOSE[7484][C-00000000] pbx.c: Executing [s@app-announcement-1:5] Playback("SIP/merionet-1-
00000000", "custom/nonworking,noanswer") in new stack
[2016-07-03 22:14:18] VERBOSE[7484][C-00000000] file.c: <SIP/merionet-1-00000000> Playing 'custom/nonworking.slin'
```

Однако, данный модуль мало полезен, если требуется проверить не только недавние логи, но и недельной, а то и месячной давности. Если появилась такая нужда, требуется подключиться к вашей АТС по SSH, например, используя терминальный клиент PuTTY. Кроме того, если есть физический доступ к серверу, можно использовать и его. Почему проще использовать терминальный клиент? Ответ прост – PuTTY поддерживает операции копировать\вставить, что многократно упрощает работу.

Просмотр логов через консоль

Итак, порядок действий для доступа к логам Астериск:

1. Вход на АТС, используя рутовый логин и пароль. После успешного входа вводится команда **cd /var/log/asterisk**
2. Для вывода списка лог-файлов нужно ввести команду **ls -l**

Обычно, все файлы называются «full-DATE», где DATE – дата логирования.

Если требуется посмотреть и отсеять сегодняшний лог-файлы, нужно ввести **nano full**. Данная команда откроет лог-файл с помощью текстового редактора nano. Nano сразу же продемонстрирует список команд для управления текстовым редактором

```
root@localhost:/var/log/asterisk
GNU nano 2.0.9 File: full
[2016-07-03 03:20:03] Asterisk 13.7.1 built by mockbuild @ jenkins2.schmoozecom.net on a i686 running Linux c
[2016-07-03 03:20:03] VERBOSE[10048] config.c: Parsing '/etc/asterisk/logger.conf': Found
[2016-07-03 03:20:03] VERBOSE[10048] config.c: Parsing '/etc/asterisk/logger_general_additional.conf': Found
[2016-07-03 03:20:03] VERBOSE[10048] config.c: Parsing '/etc/asterisk/logger_general_custom.conf': Found
[2016-07-03 03:20:03] VERBOSE[10048] config.c: Parsing '/etc/asterisk/logger_logfiles_additional.conf': Found
[2016-07-03 03:20:03] VERBOSE[10048] config.c: Parsing '/etc/asterisk/logger_logfiles_custom.conf': Found
[2016-07-03 03:20:03] VERBOSE[10048] logger.c: Asterisk Queue Logger restarted
[2016-07-03 03:20:03] VERBOSE[10048] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:22:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:22:01] VERBOSE[10510] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:22:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:24:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:24:01] VERBOSE[10765] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:24:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:24:01] VERBOSE[10774] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:26:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:26:01] VERBOSE[11025] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:26:02] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:26:02] VERBOSE[11034] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:28:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:28:01] VERBOSE[11234] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:28:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:28:01] VERBOSE[11243] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:30:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:30:01] VERBOSE[11501] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:30:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
[2016-07-03 03:30:01] VERBOSE[11506] asterisk.c: Remote UNIX connection disconnected
[2016-07-03 03:30:01] VERBOSE[3062] asterisk.c: Remote UNIX connection
^G Get Help      ^O WriteOut      ^R Read File     ^Y Prev Page     ^K Cut Text      ^C Cur Pos
^X Exit          ^J Justify       ^W Where Is      ^V Next Page     ^U UnCut Text    ^T To Spell
```


Для просмотра можно использовать клавиши Page Up и Page Down, CTRL-W для поиска и CTRL-X для выхода. Соответственно, для открытия конкретного файла, нужно написать **nano full-20160629**

Если вы случайно внесли изменения и пересохранили лог-файл, то Астериск прекратит логирование сегодняшнего дня. Для исправления данной проблемы необходимо запустить следующую команду **amportal restart**. Данная команда будет ждать 120 секунд для завершения текущих вызовов, и по прошествии 120 секунд все вызовы будут принудительно завершены.

Так же возможно использовать команду Linux grep, например для вывода в текущем лог-файле всех событий связанных с недоступным транком - grep "is now" full

- Если результатов слишком много, есть возможность скопировать их в новый файл - **grep "is now" full > newlogfile**
- Для его просмотра можно использовать уже знакомый редактор nano - **nano newlogfile**
- Удалить данный файл можно командой - **rm tempfile**
- Так же есть возможность просматривать логи в реальном времени - **asterisk -r**
- Для выхода используется команда - **exit**
- И ещё один способ просмотра лог-файлов в реальном времени – tail. Делает это так:
cd /var/log/asterisk tail -f full

Для выхода нужно нажать CTRL-C.

Проблемы со слышимостью в Asterisk

Одной из распространенных проблем, с которыми сталкивается администратор IP – АТС Asterisk является проблема с аудио. Вы можете столкнуться как с односторонней слышимостью, так и с полным отсутствием аудио – потока. Как решить проблему с аудио в Asterisk с помощью FreePBX расскажем в разделе.

Проблемы с NAT

В подавляющем большинстве случаев проблемы с односторонней слышимостью вызваны настройками [NAT \(Network Address Translation\)](#). Ниже указаны шаги, выполнение которых поможет вам избавиться от проблем с аудио

Динамический DNS

Если ваша компания не оплачивает провайдеру услугу статического IP – адреса, то ваш внешний IP будет периодически меняться. Причиной может быть перезагрузка маршрутизатора или, например, истечение срока аренды адреса по протоколу DHCP (**DHCP Lease Time**). Отличной альтернативной будет динамическая DNS запись. Данная запись позволяет серверу DNS периодически обновлять соответствующий доменному имени IP – адрес. Вне зависимости от смены IP вашим провайдером, маршрутизатор будет всегда доступен по его доменному имени. Такие услуги предоставляет такие сервисы как dyndns, no-ip, hldns и другие.

Настройка NAT В FreePBX

Когда вы приобрели статический IP – адрес или сделали динамическую запись на DNS сервере, переходим к настройке NAT. Перейдите во вкладку **Settings -> Asterisk SIP settings -> Chan SIP Settings**

The screenshot shows the 'SIP Settings' page in FreePBX. The 'Chan SIP Settings' tab is selected. Under 'Edit Settings', the 'NAT Settings' section is expanded. The 'NAT' option is set to 'yes'. The 'IP Configuration' section has three buttons: 'Public IP', 'Static IP' (which is highlighted with a blue border), and 'Dynamic IP'. Below this, the 'Override External IP' field is visible with a red border and the placeholder text 'Enter IP Address'.

На указанном выше примере, выбрана опция **Static IP**. Здесь, в выделенном красным поле необходимо указать ваш внешний IP – адрес. На примере ниже, указана опция настройки динамического **DNS** – выбрана кнопка Dynamic IP:

The screenshot shows the 'SIP Settings' page in FreePBX. The 'Chan SIP Settings' tab is selected. Under 'Edit Settings', the 'NAT Settings' section is expanded. The 'NAT' option is set to 'yes'. The 'IP Configuration' section has three buttons: 'Public IP', 'Static IP', and 'Dynamic IP' (which is highlighted with a blue border). Below this, the 'Dynamic Host' field is visible with a red border and the value 'merionet.dyndns.net'. The 'Dynamic Host Refresh' field has the value '120'.

Локальные сети

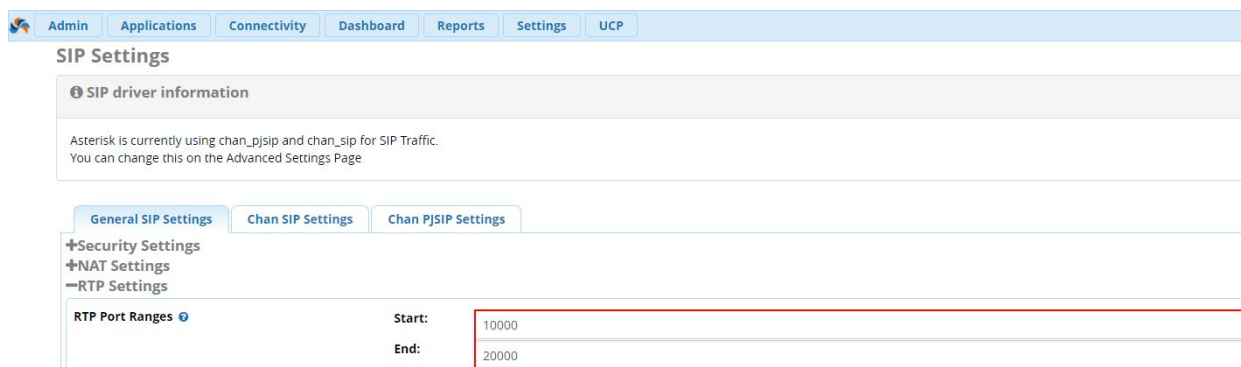
Перейдя во вкладку **General SIP Settings** того же раздела, необходимо настроить внутренние сети. Например, 192.168.13.0/255.255.255.0. Это может быть отдельная сеть, в которой находятся IP – телефоны, или сеть, в которую вынесено все активное сетевое оборудование.



Не забывайте по окончании настроек нажать **Submit** и **Apply Config**

Настройка RTP портов

Проверьте чтобы на вашем маршрутизаторе не были заблокированы UDP порты 5060 (SIP) и диапазон портов **10000-20000 (RTP)**. Помимо этого, вы можете сделать проброс этих портов прямо на ваш сервер IP – ATC Asterisk. Перепроверьте, что транспортным протоколом является именно **UDP**.



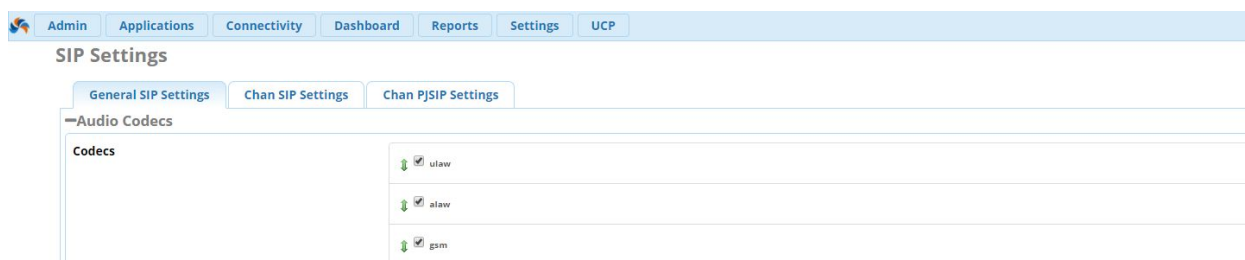
Проблемы с настройкой кодеков

Каждый раз, когда вы совершаете вызов, обе стороны, иницирующая и принимающая вызов согласует [телефонный кодек](#). Например, одна из сторон может инициировать согласование кодека g.711u, который может не поддерживаться другой стороной. Это может являться причиной отсутствия аудио в разговоре. Мы рекомендуем всегда включать поддержку кодеков G.711 u – закона и a – закона. Настроить телефонные кодеки можно следующими способами:

1. Настройка на конкретном телефонном аппарате
2. В настройка внутреннего номера (Extension) в FreePBX

Мы рекомендуем не настраивать кодеки индивидуально на телефонном аппарате. В случае возникновения каких – либо проблем, на этапе «**траблшутинга**» вы можете потратить лишнее время просто забыв о данной настройке

3. На этапе настройки SIP – транка в FreePBX. Разрешенные или запрещенные кодеки определяются опцией **allow/disallow**
4. Глобальная настройка. В разделе **Settings -> Asterisk SIP Settings -> "General SIP Settings"**



Проблема с воспроизведением аудио файлов

Если при звонке на голосовое меню (IVR) вы не слышите ожидаемую аудио – запись, проверьте, корректно ли был импортирован этот файл через модуль System Recordings. Помимо этого проверьте права этого файла. Владелец этого файла (owner) должен быть пользователь asterisk. В рамках решения проблемы дайте команду amportal **chown**:

```
[root@localhost ~]# amportal chown
Please wait...
!!!!amportal is depreciated. Please use fwconsole!!!!
forwarding all commands to 'fwconsole'
Taking too long? Customize the chown command, See
http://wiki.freepbx.org/display/FOP/FreePBX+Chown+Conf
Setting Permissions...
37034/37034 [=====] 100%
Finished setting permissions
```

Sngrep: установка и использование

Если кратко, то sngrep позволяет отображать потоки SIP – вызова (sip flow) прямо в консоли твоего сервера. Утилита покажет SIP – обмен сообщениями в удобной и читаемой форме. Скажем так: sngrep это tcpdump (или wireshark под Linux), но только для VoIP :)

Установка на CentOS

Рассмотрим быструю установку утилиты на операционной системе CentOS. Первым делом добавим **irontec** репозиторий. Для этого, создадим файл с именем **sngrep.repo** в директории **/etc/yum.repos.d**:

```
touch /etc/yum.repos.d/sngrep.repo
```

Добавляем в файл следующие строки:

```
[irontec]
name=Irontec RPMs repository
baseurl=http://packages.irontec.com/centos/$releasever/$basearch/
```

Затем импортируем публичный ключ от **irontec**:

```
rpm --import http://packages.irontec.com/public.key
```

Все готово к установке. Даем следующие команды:

```
yum update
yum install sngrep
```

По окончании установки, в командной строке дайте команду **sngrep**. Теперь давайте разберемся с функционалом и тем как пользоваться утилитой.

Использование sngrep

Как только вы попадете в меню управления утилитой, перед вами будет отражен список VoIP пакетов, которые обрабатывает Ваш сервер:

Помимо прочего, есть возможность отмечать типы сообщения, такие как REGISTER, INVITE, OPTIONS и прочие;

- **F8** - показать настройки, среди которых подсветка синтаксиса, фон и прочие;
- **F10** - настройка отображаемых параметров (такие как From/TO, индекс, метод и прочие);
- **Esc** - выйти из sngrep/в предыдущее меню;
- **Enter** - посмотреть call-flow выбранного пакета;
- **Space** (пробел) - выделить нужный сегмент;
- **i/I** - фильтрация только по сообщениям типа INVITE;
- **p** - поставить на паузу сбор пакетов;

Домашнее задание №5

В окончании пятого блока обучения, ваша задача заключается в следующем:

- У вас настроена отправка писем через **Asterisk** (уведомления). Но письма не приходят. Какой лог нужно посмотреть в первую очередь?
- Вы звоните по SIP на городской номер. Вы слышите абонента, а он вас нет. Где находится первая точка, где логичнее всего снять сетевой дамп и проанализировать наличие **RTP**?
- Установите на своем лабораторном стенде sngrep. Выполните несколько вызовов. В дампе найдите:
 - Выполненный вами звонок;
 - Какой кодек согласовали участники звонка [по SDP](#)?
 - Посмотрите какие порты **RTP** согласованы во время звонка?
 - Скачайте дамп и сохраните его локально.