

Общие команды



Успешно сдайте бесплатный сертификационный экзамен в Академии "Инфинет" и получите статус сертифицированного инженера Инфинет.

[Пройти сертификационный экзамен](#)

- [help](#)
- [system](#)
- [config](#)
- [set](#)
- [flashnet](#)
- [restart](#)
- [ping](#)
- [telnet](#)
- [tracert](#)
- [webcfg](#)
- [rshd](#)
- [ipstat](#)
- [sflowagent](#)
- [acl](#)
- [sntp](#)
- [date](#)
- [erp](#)
- [aaa \(контроль доступа посредством сервера RADIUS\)](#)
- [license](#)
- [dport](#)
- [mem](#)
- [grep](#)
- [gps](#)
- [tsync](#)
- [Протокол SSH](#)
 - [sshd](#)
 - [sshc](#)
 - [sshtun](#)
- [nslookup](#)
- [DNSclient](#)
- [cron](#)

help

Выводит список всех команд маршрутизатора.

Синтаксис:

```
help
```

system

Служит для просмотра и установки системных параметров.

Синтаксис:

```

sys [args...]
args are:
  user [Login]
  password [Password]
  [no]useAAA
  [no]useLocalAAA
  contact [String]
  guest [guest login]
  name [System Name]
  prompt [any_word]
  location [String]
  mgmtAccount [user:pass@host]
  gpsxy XX.XXXXX YY.YYYYY
  log {on|off} | {show [offset] | clear}| [no]filter | {ADDR | -}
  factorypassword {single|otp}
  search [seconds]
  [no]indicator
  [no]fastroute
  [no]mintgateway
  [no]authFailLog
  [no]sendredirects
  [no]dropredirects
  OfficialAddress X.X.X.X | 0
  icmplimit N [200]
  uptime
  cpu
  [no]pager
  [no]ipforwarding
  info [-f] [NAME]
  version

```

Параметр	Описание
<i>user [Login]</i>	Имя пользователя. Используется для доступа к устройству в привилегированном режиме. system user root
<i>password [Password]</i>	Пароль для доступа к устройству в привилегированном режиме. system password qwerty Для удаления пользователя в привилегированном режиме воспользуйтесь командой "setpass".
<i>[no]useAAA</i>	Включение/отключение контроля доступа на устройство с помощью сервера RADIUS. Для функционирования необходимо запустить модуль "AAA" (см. AAA (контроль доступа посредством RADIUS сервера)). Помните, что при аутентификации приоритет отдается серверу RADIUS. Если учетная запись не найдена посредством RADIUS, то проверяется соответствие локальной учетной записи. При отсутствии локальной учетной записи, доступ на устройство будет возможен под любым именем пользователя и паролем, даже несмотря на включенную аутентификацию через "AAA".
<i>[no] useLocalAAA</i>	Меняет приоритет аутентификации, сначала проверяется соответствие локальной учетной записи, при её отсутствии аутентификация осуществляется посредством RADIUS.
<i>contact [String]</i>	Контактные данные. system contact Russia, Yekaterinburg

guest [guest login]	Имя пользователя. Используется для доступа к устройству в непривилегированном (гостевом) режиме, может использоваться любой пароль. В этом режиме невозможно изменить настройки устройства и посмотреть параметры, влияющие на безопасность. <pre>system guest for_members_only</pre> Для удаления пользователя в гостевом режиме воспользуйтесь командой "<i>system noguest</i>".
name [System Name]	Имя устройства, которое будет отображаться в названии вкладки браузера веб-интерфейса.
prompt [any_word]	Позволяет изменить приглашение (prompt) клавиатурного монитора. Допустим любое слово до 16 букв. <pre>system prompt MyHost</pre>
location [String]	Местонахождение устройства. <pre>system location " "</pre>
mgmtAccount [user: pass@host]	Атрибуты доступа к серверу обновления программного обеспечения через протокол SNMP. <pre>system mgmtAccount [aaa:bbb@192.168.1.1]</pre>
gpsxy XX.XXXXX YY.YYYYY	Координаты места установки устройства в формате GPS, долгота и широта. <pre>system gpsxy 60.40056 56.82857</pre>
log {on off} / {show offset} / clear} [no] filter / {ADDR / -}	Управление системным журналом событий: • "on" – выводить сообщения на текущую консоль. • "off" – отключить вывод сообщений на консоль. • "show" – показать системный архив сообщений (время в секундах/миллисекундах от текущего). • "clear" – очистить архив сообщений. • "[no]filter" – удалить из системного журнала одинаковые соседние строки, оставляя только один экземпляр каждого сообщения и счётчик их повторений (по умолчанию включена). • "ADDR" – указать адрес UNIX машины для передачи сообщений в системный журнал по протоколу "syslog". В настройках сервера "syslogd" для регистрации сообщений необходимо указать "facility.level" равным "user.notice" или просто числовое значение 15. • "-" – отключить регистрацию на удалённой машине.
factorypassword {single otp}	Установка режима доступа на устройство с заводским паролем. По умолчанию каждое устройство имеет свой постоянный уникальный заводской пароль (режим "single"). Однако при необходимости этот пароль можно сделать одноразовым. В режиме "otp" устройство будет запрашивать новый пароль при каждой попытке входа с заводскими реквизитами (каждый раз будет предоставляться новый "sequence" для запроса). При переходе из режима "otp" в режим "single" постоянный пароль доступа будет восстановлен.
search [seconds]	Включение режима, в котором мигает вся световая индикация устройства для его поиска среди группы однотипных. По умолчанию режим отключается через 10 секунд.
[no] indicator	Включение/отключение внешних световых индикаторов на корпусе устройства, для того чтобы уменьшить его видимость.
[no] fastroute	Включение/отключение режима ускоренной маршрутизации. В этом режиме устройство становится невидимым для средств трассировки сети (<i>traceroute</i>), но при этом выполняет все функции маршрутизатора. Не рекомендуется включать эту опцию одновременно на нескольких устройствах, если они находятся в одном сегменте Ethernet, поскольку это может вызвать шторм IP-пакетов.
[no] mintgateway	Позволяет использовать в качестве шлюза по умолчанию (default gateway) ближайший узел MINT, который сконфигурирован с опцией "mint extg", если такой имеется.

[no] authFailLog	Включение/отключение регистрации неуспешных попыток аутентификации доступа к устройству в системном журнале.
[no] sendredirects	Включение/отключение способности системы отправлять сообщения " <i>icmp redirect</i> " для подавления источника пакетов при неправильно настроенной маршрутизации.
[no] dropredirects	Включение/отключение способности системы принимать сообщения " <i>icmp redirect</i> " для корректировки маршрутных таблиц при неправильно настроенной маршрутизации.
OfficialAddress X.X.X.X / 0	Установка адреса, который будет использоваться в качестве источника во всех исходящих с устройства соединениях. Аргумент "0" удаляет текущее значение адреса.
icmplimit N [200]	Установка ограничения на количество исходящих пакетов ICMP в секунду (по умолчанию 0). Позволяет избежать перегрузки устройства при работе программ сканирования сети. При установке в значение 0, все ограничения отключаются.
uptime	Время работы системы с момента последней перезагрузки.
cpu	Текущая загрузка центрального процессора в процентах за несколько интервалов времени.
[no]pager	Включение/отключение разбивки консольного вывода на страницы (экраны).
[no] ipforwarding	Включение/отключение IP Forwarding.
info [-f] [NAME]	Вывод информации об устройстве: • "-f" – полная информация. • "NAME" – информация по интересующему разделу.
version	Вывод информации о текущей версии программного обеспечения.

**ВНИМАНИЕ**

Любой строковый параметр можно удалить задав значение "-". Установка и отмена любых параметров может быть сохранена в постоянной конфигурации командой "*config save*".

config

Манипуляции с конфигурацией.

Синтаксис:

```
config [show [Keywords ...] | save | clear]
config {import | export} login:password@host/file
show - show current configuration
save - store current configuration to flash
clear - clear configuration in flash
import - import configuration from file
export - export configuration to file
-----
backup [list] - show list of backups
backup save N "Comment" - create configuration backup number N [1..8]
backup replace N "Text" - replace configuration backup number N
backup restore N - restore backup number N
backup del N - delete backup number N
backup show N - view text of backup number N
backup comment N "Comment" - change comment for backup N
backup {import | export} N ftp://login:password@host/file
```

Параметр	Описание
----------	----------

show	Вывод информации о текущей конфигурации системы. Любое действие по изменению параметров системы немедленно отображается в результатах команды "<i>config show</i>". Однако все изменения действительны только в течение текущего сеанса работы (до первой перезагрузки). В качестве дополнительных аргументов можно указывать начальные буквы системных команд. Пример: Конфигурация протоколов MINT и RIP: <pre>co show mint rip</pre> Конфигурация всех команд, начинающихся на "r", кроме "rip": <pre>co show r !rip</pre>
diff	Выводит все изменения внесённые в конфигурацию с момента её последнего сохранения.
save	Сохранение текущей конфигурации системы в энергонезависимую память маршрутизатора для последующего постоянного использования. При вводе данной команды предыдущая конфигурация автоматически сохраняется в качестве резервной с номером записи 0.
clear	Сброс конфигурации устройства (устанавливает заводскую конфигурацию по умолчанию). После ввода команды необходимо перезагрузить устройство.
import	Загрузка конфигурации маршрутизатора с удалённого сервера. Операция выполняется по протоколу FTP. Файл должен быть задан полным именем в формате используемой файловой системы.
export	Сохранение конфигурации маршрутизатора на удалённом сервере. Операция выполняется по протоколу FTP. Файл должен быть задан полным именем в формате используемой файловой системы. <pre>config export user:secret@192.168.1.1/var/conf/test.cfg</pre>
backup [list]	Вывод резервного списка конфигурации.
backup save N "Comment"	Создание резервной конфигурации с номером N (1 ... 8).
backup replace N "Text"	Замена старой резервной конфигурации на новую.
backup restore N	Восстановление резервной конфигурации N.
backup del N	Удаление резервной конфигурации N.
backup show N	Просмотр резервной конфигурации N.
backup comment N "Comment"	Изменение описания резервной конфигурации N.
backup {import export} N ftp://login:password@host /file	Импорт/экспорт резервной конфигурации на ftp-сервер.

set

Команда применяется для установки временной зоны, поддерживает автоматический переход на летнее/зимнее время.

**ВНИМАНИЕ**

Временная зона определяется на устройстве Master и автоматически распространяется на все устройства, подключенные непосредственно к нему. Таким образом, если на устройствах Slave установлена иная временная зона, то она будет переопределена на ту, которая установлена на устройстве Master.

Синтаксис:

```
set TZ TIMEZONE
```

Параметр	Описание
TIMEZONE	Временная зона, указывается в формате POSIX: <pre>std offset [dst] [offset],start[/time],end[/time]</pre> "<i>std offset</i>" – имя временной зоны и время offset, которое должно быть добавлено, чтобы результатом было значение времени UTC. Если указаны только эти параметры, то временная зона будет применена без учета перехода на летнее время. Следующие параметры являются необязательными и должны применяться в том случае, если требуется обеспечить автоматический переход на летнее время. "<i>[dst] [offset]</i>" – имя временной зоны и разница с UTC для летнего времени. "<i>start[/time],end[/time]</i>" – день и время начала и завершения периода, когда применяется летнее время. Значение "<i>start</i>" и "<i>end</i>" указывается в формате "<i>Mm.n.d</i>": "<i>Mm</i>" – месяц, от 1 до 12; "<i>d</i>" – день недели, от 0 до 6, где 0 – воскресенье; "<i>n</i>" – неделя в месяце, от 1 до 5, где 1 – первая неделя, 5 – последняя. Более подробную информацию о формате указания временной зоны вы можете прочитать в соответствующей статье: http://www.gnu.org/software/libc/manual/html_node/TZ-Variable.html

Пример:

```
set TZ EST+5EDT,M4.1.0/2,M10.5.0/2
set TZ EKT+5
```

**ВНИМАНИЕ**

Более подробно о формате установки часового пояса описано в статье http://ru.wikipedia.org/wiki/Часовой_пояс.

flashnet

Загрузка/выгрузка программного обеспечения.

Синтаксис:

```
flashnet get|put login:password@host/file [-S src_addr]
```

Параметр	Описание
----------	----------

get	Загрузка на устройство новой версии программного обеспечения. Загрузка выполняется по протоколу FTP. В качестве имени файла следует указать полное имя в формате используемой файловой системы. Процесс загрузки делится на две фазы: • Считывание файла с удалённого сервера и проверка его целостности. • Запись образа системы в память маршрутизатора. Вторая фаза отображается на экране повторяющимся знаком ".". Для обновления с официального ftp-сервера компании "Инфинет", используйте команду: <pre>flashnet get ftp:ftp@ftp://91.191.225.246/firmware.H11S01v1.6.6.bin</pre> где • "H11" – аппаратная платформа. • "1.6.6" – версия программного обеспечения. • "ftp" – имя пользователя. • "ftp" – пароль.  ВНИМАНИЕ После установки нового программного обеспечения, устройство необходимо перезагрузить командой: <pre>restart yes</pre>
put	Выгрузка программного обеспечения на внешний сервер.
-S	С помощью этой опции можно подставить любой IP-адрес источника.

restart

Команда выполняет полную перезагрузку и переинициализацию устройства также как и в случае повторного включения питания.

Может быть использована для восстановления исходной конфигурации после серии безуспешных попыток понять, что именно сделано не так, а также после загрузки новой версии программного обеспечения.

Синтаксис:

```
restart [y] | [SECONDS] | [stop]
```

Параметр	Описание
y	Перезагрузка выполняется сразу без запроса подтверждения.
SECONDS	Время, на которое отложена перезагрузка устройства, в секундах. Это может быть полезно в случае проведения рискованных манипуляций с конфигурацией, когда есть опасность потерять контроль над устройством. Система будет периодически предупреждать об оставшемся времени до перезагрузки сообщением в системный журнал. Повторное выполнение команды начинает отсчёт времени сначала.
stop	Отмена отложенной перезагрузки.

ping

Посылает тестовые пакеты ("ICMP_ECHO_REQUEST") на заданный IP-адрес. Позволяет оценить достижимость и время отклика прохождения пакетов.

Синтаксис:

```
ping IP [-s size_in_bytes] [-c count_packets] [-S IP] [-t sec] [-q] [-l]
```

Параметр	Описание
-s <i>size_in_bytes</i>	Длина тестового пакета в диапазоне от 10 до 8000 байт, по умолчанию 56.
-c <i>count_packets</i>	Количество отправляемых запросов, по умолчанию 5.
-S IP	Используемый IP-адрес источника. По умолчанию, в качестве адреса источника подставляется адрес интерфейса, через который отправляются пакеты.
-t sec	Интервал отправки запросов, в секундах. Возможны дробные значения, по умолчанию 1 секунда.
-q	Тихий (quiet) режим. Вывод только итоговой статистики.
-l	Тихий (quiet) режим с отображением потерянных (lost) пакетов.

telnet

Команда используется для установки соединения с удалённым устройством в режиме эмуляции терминала. В данной реализации используется простая прозрачная трансляция потока символов без какой-либо промежуточной интерпретации, поэтому тип терминала будет определяться тем терминалом, с которого была выполнена данная команда. Аварийное прерывание сеанса выполняется при нажатии клавиш "Ctrl/D".

Синтаксис:

```
telnet address [port] [-S source]
```

Параметр	Описание
port	Порт Telnet.
-S source	IP-адрес устройства.

tracert

Трассирует путь прохождения пакетов до заданного узла (host). Команда использует различные значения поля протокола IP "time to live" в исходящих пакетах и анализирует ответы "ICMP TIME_EXCEEDED", поступающие от всех маршрутизаторов, находящихся на пути к выбранному узлу. По умолчанию, в качестве адреса источника подставляется адрес интерфейса, через который отправляются пакеты. С помощью опции "-S" можно подставить любой другой IP-адрес. Трассировка ограничивается 30-ю промежуточными узлами. Длина отправляемых пакетов равна 40 байтам. Для каждого промежуточного узла выполняется 3 попытки. Результат трассировки содержит адрес промежуточного маршрутизатора и время отклика для каждой попытки в миллисекундах.

Синтаксис:

```
tracert host [-S src_addr]
```

Параметр	Описание
-S src_addr	IP-адрес узла.

**ВНИМАНИЕ**

Кроме того, могут появляться специальные символы, отображающие коды специфических ответов протокола ICMP:

- "!" – порт недоступен.
- "!N" – сеть недоступна.
- "!H" – узел недоступен.
- "!P" – недопустимый протокол.
- "!F" – пакет превышает допустимую длину.
- "!X" – административный запрет на доступ к узлу (фильтр, прокси, и т.д.).
- "*" – нет отклика.

webcfg

Поддержка веб-интерфейса.

Синтаксис:

```
Available commands are:
sta[rt]           Start WEBCFG service
sto[p]           Stop WEBCFG service
cmd[s]           Show additional commands added by WEBCFG
clrc[md]         Clear additional commands added by WEBCFG

Available options are:
-http={on,off}   Off if Web interface access by HTTPS only
-help -h -?      Help
-lang={en|ru|fr|it|cn} Default language at service startup
```

Параметр	Описание
<i>sta[rt]</i>	Включение поддержки веб-интерфейса на устройстве. Веб-интерфейс позволяет производить конфигурацию устройства с помощью веб-браузера.
<i>sto[p]</i>	Отключение поддержки веб-интерфейса на устройстве.
<i>cmd[s]</i>	Просмотр команд, введенных через веб-интерфейс.
<i>clrc[md]</i>	Удаление команд, введенных через веб-интерфейс.
<i>-http={on,off}</i>	Включение/отключение доступа через веб-интерфейс по HTTPS.
<i>-help -h -?</i>	Вывод списка всех аргументов команды " <i>webcfg</i> ".
<i>-lang={en ru fr it cn}</i>	Выбор языка веб-интерфейса: английский, русский, французский, итальянский, китайский.

rshd

Сервер Remote Shell (RSH) удобно использовать для периодического снятия накопленной статистики с маршрутизатора (`rsh -l mysecretuser RWR.domain.ru ipstat get`). Сервер RSH обеспечивает удалённое выполнение команд с помощью команды "*rsh*". Идентификация основана на использовании привилегированных портов TCP и списка разрешённых узлов. По умолчанию сервер RSH не активен.

Синтаксис:

```
rshd {enable | ipstat | disable} RUSER RHOST LUSER
rshd start | stop | flush | [-]log
```

Параметр	Описание
----------	----------

enable	Вход в систему с тремя параметрами: • "RUSER" – имя удалённого пользователя (до 16 символов). • "RHOST" – IP-адрес удалённого узла. • "LUSER" – имя локального пользователя (до 16 символов).
ipstat	Позволяет указанному пользователю выполнять только системную команду "ipstat".
disable	Отмена входа в систему с параметрами, указанными при входе.
start	Запуск сервера. После запуска сервер не будет обрабатывать запросы на выполнение команд, до тех пор, пока не будет определён хотя бы один разрешённый вход в систему. Запрос на выполнение команды будет выполнен только в том случае, если все три параметра в запросе совпали с заданными. Может быть указано до 6-ти независимых входов. Имя локального пользователя никак не связано с основной системой авторизации WANFleX и может рассматриваться как ключевое слово.
stop	Остановка сервера.
flush	Полный сброс конфигурации сервера RSH.
[-]log	Включение/отключение записи в системный журнал сообщений о попытках выполнить команды с помощью протокола RSH.

Пример:

```
rshd enable admin 195.38.44.1 mysecretuser
rshd enable root 195.38.45.123 mysecret2
rshd start
```

Пример снятия статистики с устройства с помощью "rsh":

```
#!/usr/bin/perl -w
for(;;)
{
    my $stat;
    do
    {
        $stat = system("rsh -t 30 -n -l root IWR_IP
ips fixit >/dev/null");
        if(int($stat) != 0) { sleep(5); }
    } while (int($stat) != 0);
    do
    {
        $stat = system("rsh -t 30 -n -l root IWR_IP
ips fixget >stat.tmp");
        if(int($stat) != 0) { sleep(5); }
    } while (int($stat) != 0);
    do
    {
        $stat = system("rsh -t 30 -n -l root IWR_IP
ips fixclear >/dev/null");
        if(int($stat) != 0) { sleep(5); }
    } while (int($stat) != 0);

    system("cat stat.tmp >>stat.txt");

    sleep(300);
}
```

ipstat

Модуль сбора статистики IP. Модуль статистики позволяет накапливать информацию о проходящих через маршрутизатор потоках данных для последующего анализа и/или тарификации. Накапливаемые данные хранятся в оперативной памяти маршрутизатора в виде записей с полями: адрес источника, адрес получателя, количество переданных байт, Кбит/с и пакетов/с. По умолчанию считаются только исходящие пакеты в момент отправки через какой-либо физический интерфейс.

Синтаксис:

```
ipstat enable [incoming|outgoing|full] [detail] [SLOTS] | disable
ipstat clear
ipstat traf [detail] [speed | total_bytes | pps] [reverse] [[if=IFNAME] [swg=N] -f "PCAP"]
ipstat fixit | fixget | fixclear
ipstat strict | -strict
ipstat add [intf] [swg=N] -f "PCAP"
ipstat del num
ipstat rearrange [N]
```

Параметр	Описание
enable [incoming outgoing full] [detail] [SLOTS] disable	Включение/отключение сбора IP-статистики: "incoming/outgoing" – позволяют считать только входящие/исходящие пакеты. "full" – включает режим обработки входящих и исходящих потоков данных. "detail" – включает сбор расширенной статистики, включая информацию по портам и протоколам. "SLOTS" – позволяет установить максимальное количество записей в таблице данных "ipstat". По умолчанию число записей – 1000, этого количества обычно хватает на 15-20 минут на обычном абонентском терминале. Каждая запись занимает 12 байт.
clear	Очистка накопленной статистики.
traf [detail] [speed total_bytes pps] [reverse] [[if=IFNAME] [swg=N] -f "PCAP"]	Просмотр процесса накопления статистики в реальном времени: "detail" – включает сбор расширенной статистики, в том числе информацию по портам и протоколам. "speed" – сортирует вывод команды по скорости передачи. "total_bytes" – сортирует вывод команды по количеству переданных байт за весь период. "pps" – сортирует вывод команды по количеству переданных пакетов в секунду. "reverse" – позволяет выполнять сортировку по указанному критерию (speed total_bytes pps) в обратном порядке. "if=IFNAME" – вывод статистики по указанному порту. "swg=N" – вывод статистики по указанной группе коммутации. "-f "PCAP" – вывод статистики по указанному фильтру выражения rpsar.
fixit	Сброс текущей статистики в промежуточный буфер. Текущая статистика обнуляется и начинает накапливаться заново.
fixget	Отображение содержимого сохранённого сброса статистики. Эту команду можно выполнять неограниченное количество раз без потери текущей статистики.
fixclear	Очистка временного сброса статистики.
strict -strict	В случае переполнения таблицы записей или нехватки памяти, в системный журнал выводится соответствующее предупреждение и вновь поступающие данные не учитываются в статистике. Если включена опция "strict", то при возникновении такой ситуации на устройстве отключается сквозная маршрутизация. При этом само устройство остаётся доступным по любому протоколу.
add [intf] [swg=N] -f "PCAP"	Ограничение числа пакетов, попадающих в статистику, только теми, которые удовлетворяют добавленному правилу: "intf" – имя интерфейса, через который пакет попадает в систему. "swg=N" – принимает пакеты, относящиеся к группе коммутации N. "-f "PCAP" – фильтр выражений rpsar.  ВНИМАНИЕ Синтаксис правил полностью соответствует синтаксису команды "ipfw".

<i>del num</i>	Удаление правила из списка.
<i>rearrange [N]</i>	Перенумерация всех правил в списке с заданным шагом N (по умолчанию шаг равен 1).

sflowagent

Реализация протокола Sflow. Sflow – это протокол, предназначенный для мониторинга компьютерных сетей. Он так же используется провайдерами для снятия информации об использовании предоставляемых сервисов абонентами.

Синтаксис:

Available commands are:

```
sta[rt]           Start Sflow agent
sto[p]           Stop Sflow agent
wi[pe]           Stop Sflow agent and clean all configuration
add[instance] 'name' Add instance (default 'ipstat')
del[instance] 'name' Delete instance (default 'ipstat')
stat 'name'       Show statistics for instance (default 'ipstat')
cl[earstat] 'name' Clear statistics for instance (default 'ipstat')
```

Available options are:

```
-collector=IPaddress[:port] Set collector address (default 0.0.0.0:6343 )
-agent=IPaddress           Set agent address (default 0.0.0.0)
-maxpacket=size            Set maximal datagram size (default 1472)
-interval=number           Set statistics receive interval, in seconds (default 15)
-datagrams=number          Set datagrams per statistics interval (default 100)
-rawheader={on|off}        Send packets raw header instead IPv4 data (default off)
-debug={on|off}            Display debug output (default off)
-version -v                Display Version
```

Параметр	Описание
<i>sta[rt]</i>	Запуск агента Sflow.
<i>sto[p]</i>	Остановка агента Sflow.
<i>wi[pe]</i>	Остановка агента Sflow и удаление его конфигурации.
<i>add [instance] 'name'</i>	Добавление компоненты сбора статистики (по умолчанию " <i>ipstat</i> ").
<i>del [instance] 'name'</i>	Удаление компоненты сбора статистики (по умолчанию " <i>ipstat</i> ").
<i>stat 'name'</i>	Отображение статистики для определенной компоненты (по умолчанию " <i>ipstat</i> ").
<i>cl[earstat] 'name'</i>	Удаление статистики для определенной компоненты (по умолчанию " <i>ipstat</i> ").
<i>- collector=IP address[: port]</i>	Установка адреса коллектора, обрабатывающего пакеты Sflow. Порт по умолчанию 6343.
<i>- agent=IP address</i>	Установка собственного адреса агента (устройства).
<i>- maxpacket= size</i>	Установка максимального размера пакета Sflow в байтах. По умолчанию 1472 байта. Верхний предел ограничен возможностями "железа" и операционной системы. В случае его превышения размер пакета будет, соответственно, уменьшен до приемлемого значения.

- <i>interval=number</i>	Время в секундах, равное интервалу, с которым производится получение накопленной статистики из " <i>instance</i> ". Увеличение этого параметра приводит к повышению общего КПД системы, но в случае внезапного увеличения активности в сети при его слишком больших значениях данные могут пропасть. По умолчанию 15 с.
- <i>datagrams=number</i>	Максимальное число датаграмм за время между получениями статистики из " <i>instance</i> ". Увеличение этого параметра приводит к уменьшению среднего размера датаграммы и увеличивает теоретическое количество пересылаемых статистических данных, уменьшает нагрузку на CPU. Но, в то же время, уменьшает общий КПД системы. Однако, уменьшение КПД системы не происходит при небольшом трафике, т.к. датаграммы создаются по мере необходимости. Рекомендуется увеличивать при уменьшении параметра " <i>maxpacket</i> " и /или увеличении " <i>interval</i> ". По умолчанию 100. Максимальный поток " <i>sflow = datagrams/interval * maxpacket</i> ", (Б/с)
- <i>rawheader={on off}</i>	Отправка вместо статистических данных оригинальных заголовков пакетов IPv4 (по умолчанию - " <i>off</i> "). Используется для совместимости с различными программами учета трафика.
- <i>debug={on off}</i>	Печать диагностической информации в системный журнал.
- <i>version -v</i>	Текущая версия агента Sflow.

Описание параметров при выводе команды.

Параметр	Описание
<i>Cycles</i>	Общее число успешных циклов получения статистики.
<i>Overflow records</i>	Количество записей в " <i>instance</i> " в случае, когда он переполнился раньше окончания периода, заданного параметром " <i>interval</i> ".
<i>Overflow count</i>	Количество случаев, когда " <i>instance</i> " переполнился раньше окончания периода, заданного параметром " <i>interval</i> ".
<i>Samples</i>	Количество сгруппированных записей, полученных из " <i>flow records</i> ".
<i>Datagrams</i>	Общее число отправленных датаграмм.
<i>Records</i>	Число записей статистики.
<i>Bytes</i>	Общее количество переданных байт.
<i>Unused datagrams</i>	Число неиспользованных датаграмм.
<i>Dropped records</i>	Количество отброшенных датаграмм.
<i>Dropped samples</i>	Количество отброшенных записей, полученных из " <i>flow records</i> ".
<i>Pending datagrams</i>	Количество датаграмм, ожидающих в данный момент отправки.
<i>Lost flow records</i>	Отброшенное число " <i>flow records</i> " из-за низких значений параметров " <i>maxpacket</i> ", " <i>interval</i> " и " <i>datagrams</i> ".
<i>Lost overflow records</i>	Количество случаев, когда " <i>instance</i> " переполнился раньше окончания периода, заданного параметром " <i>interval</i> ", и данные были потеряны.

Пример:

```
ipstat enable full detail 3000 #
sflow add ipstat #
sflow -collector=1.2.3.4 start #
```

acl

Списки контроля доступа (Access Control Lists). В практике сетевого планирования довольно часто возникает необходимость группировки некоторых однотипных параметров для использования их в качестве списка допустимых значений различных фильтров (например, "*ipfw*", "*qm*", "*ipstat*"). Списки контроля доступа позволяют эффективно решить эту задачу.

Синтаксис:

```

acl add $NAME TYPE XXX ...
acl del $NAME [XXX ...]
acl ren $NAME1 $NAME2
acl flush
Possible TYPES: net num
Predefined ACL names:
$ACLOCAL net - Hosts (networks) permitted to access the device.
$LOCAL net - all local IPv4 addresses (only for ipfw/qm).

```

Параметр	Описание
add \$NAME TYPE XXX ...	Создание списка доступа с именем " <i>NAME</i> " и типом " <i>TYPE</i> ". Имена списков должны начинаться с символа "\$" и могут содержать до 7 алфавитно-цифровых символов, исключая пробелы и знак ";" (точка с запятой). Одновременно в команде может быть указано несколько параметров типа " <i>TYPE</i> ", которые будут помещены в созданный список. Если список с указанным именем уже существовал ранее, то перечисленные параметры будут добавлены к уже имеющемуся списку.
del \$NAME [XXX ...]	Удаление перечисленного параметра из списка " <i>NAME</i> ". Если не задано ни одного параметра, то будет удалён весь список.
ren \$NAME1 \$NAME2	Изменение имени списка с " <i>NAME1</i> " на " <i>NAME2</i> ".
flush	Удаление всех списков вместе с их содержимым.
Возможные типы списков (TYPE)	
net	Список содержит сетевые адреса в формате dot: • xxx.xxx.xxx.xxx или xxx.xxx.xxx.xxx/MASKLEN или • xxx.xxx.xxx.xxx/xxx.xxx.xxx.xxx. Список типа "<i>net</i>" оптимизирует сохраняемые параметры путём исключения дубликатов и поглощения более мелких сетей более крупными. Например, если в списке содержался параметр 1.1.1.1, то включение в него сети 1.1.1.0/24 приведёт к исключению из списка адреса 1.1.1.1. Пример: <pre> acl add \$LIST1 net 10.0.0.0/8 192.168.0.0/16 5.5.5.5 acl del \$LIST1 100.100.100.100/28 </pre>
Предопределённые имена ACL	
\$ACLOCAL net	Список IP-адресов для ограничения доступа к устройству по протоколам telnet, ssh, http/https, snmp (порты 22, 23, 80, 162, 443). При наличии списка "<i>\$ACLOCAL</i>" попытки установить соединение с устройством с адресов (сетей), не перечисленных в данном списке, будут отвергаться. Создание правил при этом не требуется. Пример: <pre> acl add \$ACLOCAL net 10.0.0.0/8 192.168.0.0/16 </pre>
\$LOCAL net	Список всех IP-адресов, назначенных данному устройству. Может быть использован для удобной записи фильтров, ограничивающих /разрешающих доступ к устройству по протоколам telnet, ssh, http/https, snmp (порты 22, 23, 80, 162, 443). Подробную информацию о настройке фильтров можно найти в статье Команда ipfw (IP Firewall) .

**ВНИМАНИЕ**

Начиная с версии ПО MINTv1.90.36 и TDMAv2.1.10 срабатывание фильтра \$ACLOCAL не фиксируется в журнале устройства, как это производилось ранее. Если необходимо включить логгирование, воспользуйтесь командой "*td log*".

sntp

Команда предназначена для управления параметрами SNTP. Наличие поддержки SNTP позволяет операционной системе WANFlex синхронизировать время с указанным сервером NTP, используя четвертую версию протокола SNTP RFC 2030. Клиент работает в режиме опроса unicast сервера в заданные промежутки времени.

Учитывая, что синхронизация времени и временной зоны обеспечивается протоколом MINT (см. команду "set"), то для синхронизации времени между устройствами сети не требуется применение протокола SNTP. Таким образом, оптимальный сценарий синхронизации выглядит следующим образом:

- 1. Ведущее устройство (Master)
 - a. Клиент SNTP включен и настроен на получение времени с корпоративного или общедоступного источника.
 - b. Сервер SNTP выключен.
- 2. Ведомое устройство (Slave)
 - a. Клиент SNTP выключен – синхронизация выполняется средствами MINT.



Начиная с версии ПО 1.90.29 в поддержке протокола SNTP произошли изменения. Теперь с помощью SNTP передается информация не только о времени, но и о временной зоне. Таким образом, больше не требуется вручную настраивать временные зоны на ведомых устройствах. Если они по протоколу SNTP синхронизируются с ведущим, то на них будет автоматически применена его временная зона.

Синтаксис:

```
sntp [options] [command]
where commands are:
  start - start service
  stop  - stop service
where options are:
  -server={ipaddr}    - set sntp server address
  -gps={on|off}       - enable/disable GPS time source
  -interval={seconds} - specify poll interval in seconds [1800]
  -supplier={on|off}  - enable/disable server mode
  -debug={on|off}     - enable/disable debug information
```

date

Управление датой и временем. Команда показывает или устанавливает дату и время в системе WANFlex. При установке даты и времени изменяется не только системное время (kernel clock), но и "hardware clock" (если такая поддержка есть в конкретном устройстве).

Синтаксис:

```
date [[[[[cc]yy]mm]dd]hh]mm[.ss]]
```

Параметр	Описание
start	Запуск процесса синхронизации времени.
stop	Остановка процесса синхронизации времени.
-server={ipaddr}	Установка IP-адреса сервера SNTP. Пример: sntp -server=9.1.1.1

-gps= {on off}	Включение/отключение источника времени GPS. В случае если к устройству подключено внешнее устройство синхронизации AUX-ODU-SYNC, то в качестве источника точного времени можно использовать встроенный приёмник ГНСС (при наличии сигналов от группировки спутников). При этом адрес внешнего сервера SNTP можно не указывать. Пример: <pre>sntp -server='ip-external-sntp-server' -gps=on</pre> Устройство в этом случае в качестве источника точного времени будет использовать как спутник, так и внешний сервер SNTP, при этом приоритетным будет источник со спутника.
-interval= {seconds}	Установка промежутка времени в секундах, через который клиент будет опрашивать сервер NTP, по умолчанию 1800. Пример: <pre>sntp -interval=5000</pre>
-supplier= {on off}	Включение/отключение поддержки серверного режима.
-debug= {on off}	Включение/отключение записи информации об отладке в журнал операционной системы WANFlex. Пример: <pre>sntp -debug=on sntp -debug=off</pre>

Параметр	Описание
cc	Век, 20 или 21.
yy	Год в сокращённом виде (например, 89 для 1989, 05 для 2005).
mm	Месяц в числовом виде от 1 до 12.
dd	День, от 1 до 31.
HH	Час, от 0 до 23.
MM	Минуты, от 0 до 59.
ss	Секунды, от 0 до 61 (59 плюс максимально две секунды координации (leap seconds)).

Пример:

```
date 201907170951.12
Wed Jul 17 09:51:12 GMT 2019 (manual)
```

```
date
Wed Jul 17 09:56:15 GMT 2019 (manual)
```

erp

Утилита ERP позволяет восстановить утерянный пароль доступа к устройству.

Синтаксис:

```

erp [options] [command]
[options]:
  -serial <n>      - device serial number
  -code <c>        - ERP code (Factory password)
  -ip <address>    - interface IP address
  -mask <mask>    - interface IP address mask

[command]:
  boot            - force continuing boot on device(s).
                   Device serial number may be unspecified
                   and means 'any device'.
  reset           - resets device's configuration.
                   Serial number and ERP code must be specified
  ifup            - turns up device's interface and adds IP address
                   and mask alias to it. Serial number, IP address
                   and IP address mask should be specified
  If command is not specified, then it's assumed the 'boot' command.

```

Параметр	Описание
-serial <n>	Серийный номер устройства.
-code <c>	Код ERP (заводской пароль).
-ip <address>	IP-адрес интерфейса Ethernet устройства.
-mask <mask>	Маска сети.
boot	Перезагрузка устройства.
reset	Сброс конфигурации устройства, имени пользователя и пароля доступа на устройство. Для выполнения команды обязательно должны быть указаны серийный номер и код ERP.
ifup	Включение интерфейса Ethernet устройства и установка на нем заданного IP-адреса и маски сети. Для выполнения команды необходимо указать серийный номер, IP-адрес и маску сети.

Для проведения процедуры восстановления пароля необходимо иметь два устройства "Инфинет". Одно устройство, на котором утерян пароль доступа, второе – на котором запускается утилита ERP. Оба устройства должны быть подключены к одному сегменту сети Ethernet через свои интерфейсы Ethernet. Следует обратить особое внимание на то, что на интерфейсе Ethernet второго устройства не должно быть опции "*switch local-tag <x>*", иначе устройства не смогут установить связь.

Порядок проведения процедуры восстановления пароля:

- Запускаем утилиту ERP с опцией "*serial*", содержащей серийный номер устройства с потерянным паролем доступа. ERP перейдет в режим ожидания заданного устройства.

```
erp -serial <SERIAL>
```

- Перезагружаем устройство, на котором утерян пароль доступа, отключением-включением питания.
- ERP покажет значение параметра "*sequence*" и серийный номер устройства с утерянным паролем. Отправляем эти значения в службу технической поддержки компании "Инфинет".
- Служба технической поддержки сообщит код ERP.
- В утилите ERP вводим команду:

```
erp -serial <SERIAL> -code < ERP> reset
```

- Снова перезагружаем устройство, на котором был утерян пароль доступа.
- Утилита ERP сбросит имя пользователя и пароль доступа на устройстве с утерянным паролем.
- Заходим на устройство с любым ненулевым именем пользователя и паролем и вводим команду:

```
config save
```

Чтобы изменить IP-адрес на интерфейсе Ethernet, не заходя на само устройство, следует выполнить следующую команду (команда может быть использована в случаях, если на устройстве отключен интерфейс Ethernet (down) или не известен IP-адрес интерфейса):

```
erp -serial <SERIAL> -ip <address> -mask <mask> ifup
```

aaa (контроль доступа посредством сервера RADIUS)

Утилита "aaa" позволяет настроить контроль доступа на устройство, используя удаленный сервер RADIUS.

Синтаксис:

```
aaa [options] [command]
where commands are:
  start - start service
  stop  - stop service
where options are:
  -auth=ip[:port],secret[,identifier] - RADIUS server parameters,
                                     address    - Server IP Address
                                     secret     - shared secret
                                     identifier - NAS Identifier
                                     this option can be repeated.
  -remove=ip[:port]                  - Remove RADIUS server.
```

Параметр	Описание
start	Запуск работы утилиты "aaa".
stop	Остановка работы утилиты "aaa".
-auth=ip[:port],secret[,identifier]	Установка параметров доступа к удаленному серверу RADIUS: "ip[:port]" – IP-адрес и порт сервера RADIUS. "secret" – пароль на сервере. "identifier" – идентификатор NAS.
-remove=ip[:port]	Удаление информации из конфигурации о сервере RADIUS.

При активации режима отладки и включенном контроле доступа на устройство посредством сервера RADIUS, в локальную консоль пользователя будет выводиться часть информации об отладке для проверки настроенных параметров.

Параметр	Описание
Request id	Системный номер запроса.
Type	Тип запроса, например, Access-Request.

Атрибуты RADIUS для запросов Access-Request и Access-Accept представлены в таблицах ниже.

Запрос Access-Request

Атрибут	Описание
1 - User-Name	Имя пользователя
2 - User-Password	Пароль пользователя
4 - NAS-IP-Address	IP-адрес сервера удаленного доступа

6 - Service-Type	Отправляется значение Login (1)
31 - Calling-Station-Id	IP-адрес подключающегося устройства
32 - NAS-Identifier	
61 - NAS-Port-Type	Отправляется значение Virtual (5)

Предусмотрена упрощенная, расширенная поддержка сервера RADIUS для идентификации беспроводных подключений:

Атрибут=Значение	Описание
1 - User-Name = "00-00-00-00-00-00"	MAC-адрес подключающегося устройства
2 - User-Password = "dummy"	Фиктивное значение
6 - Service-Type = Framed (2)	Отправляется значение Framed (2)
31 - Calling-Station-Id = "00-00-00-00-00-00"	MAC-адрес подключающегося устройства
2 - NAS-Identifier = "Infinet Base 1"	
61 - NAS-Port-Type = Wireless-802.16 (27)	Значение Wireless-802.16 (27)

Запрос Access-Accept

Атрибут	Описание
Session-Timeout	В случае если в ответе от сервера RADIUS указан параметр "Session-Timeout", то по истечении заданного времени будет отправлен новый запрос на подключение для продления или разрыва существующего канала связи. Значение: 3600 секунд.

license

Команда "*license*" служит для загрузки/выгрузки и просмотра файла лицензии на устройстве.

Синтаксис:

```
license [options]
options are:
--install=<url> - install new license
--export=<url>  - export current license to external server
--show         - show license info
<url> = ftp://[login[:password]@]host/file
```

Параметр	Описание
-install=<url>	Загрузка на устройство файла лицензии.
-export=<url>	Выгрузка с устройства файла лицензии.
-show	Вывод информации о лицензии устройства.

Пример:

```
li --export=ftp://ftp_login:ftp_password@192.168.145.1/license_file
li --show
```

dport

Title

Данная команда устанавливает битрейт для консольного порта. Допустимые значения: 9600, 19200, 38400, 57600, 115200 Бит/с. Значение по умолчанию: 38400 Бит/с.

Синтаксис:

```
dport BAUD
```

mem

Данная команда показывает статистику выделенной системной памяти устройства, сетевых буферов ("mbuf"), пакетов в очередях и отброшенных на интерфейсе пакетов.

Синтаксис:

```
mem
```

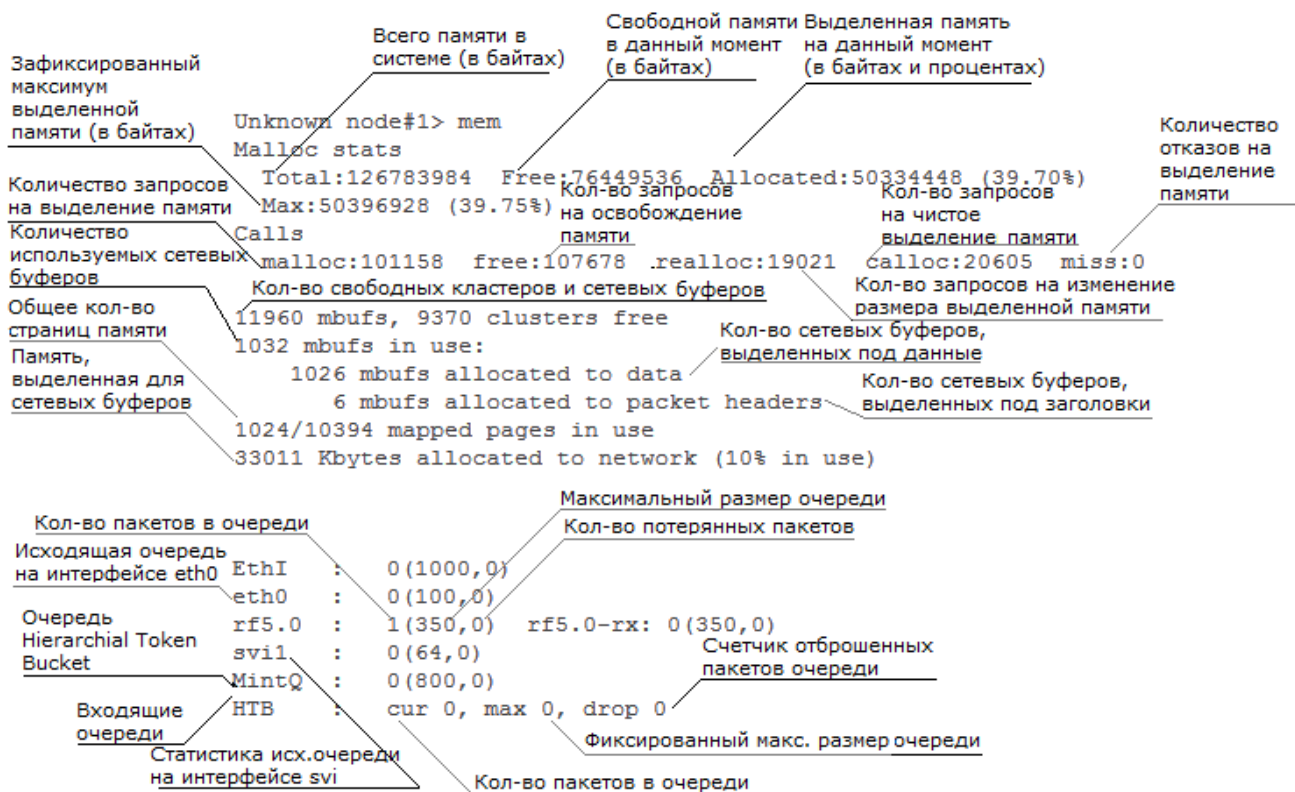


Рисунок - Пример вывода команды "mem"

grep

Команда "grep" фильтрует стандартный вывод команды (command), производя поиск и оставляя только те строки, которые содержат заданный шаблон (PATTERN).

! ПРЕДОСТЕРЕЖЕНИЕ

Данная команда недоступна на платформах H01/H02.

Синтаксис:

```
grep [OPTIONS] [-e]PATTERN "command"
or
command | grep [OPTIONS] [-e]PATTERN
```

OPTIONS:

```
-e PATTERN, --regexp=PATTERN
    Use search PATTERN possibly beginning with (-)
-i, --ignore-case
    Ignore case distinctions in PATTERN
-v, --invert-match
    Invert the sense of matching, to select non-matching lines
-w, --word-regexp
    Select only those lines containing matches that form whole words
-x, --line-regexp
    Select only those matches that exactly match the whole line
-c, --count
    Suppress normal output; instead print a count of matching lines
    With the -v, --invert-match option, count non-matching lines
-m NUM, --max-count=NUM
    Stop parsing after NUM matching lines
-n, --line-number
    Prefix each line of output with the 1-based line number
-A NUM, --after-context=NUM
    Print NUM lines of trailing context after matching lines
    Places a group separator line (--) between contiguous groups of matches
-B NUM, --before-context=NUM
    Print NUM lines of leading context before matching lines
    Places a group separator line (--) between contiguous groups of matches
-C NUM, --context=NUM
    Print output context NUM lines before and NUM lines after matching lines
    Places a group separator line (--) between contiguous groups of matches
```

Параметр	Описание
-e PATTERN, -- regexp=PATTERN	Использует шаблон поиска, начинающийся с (-).
-i, --ignore-case	Игнорирует регистр букв при поиске.
-v, --invert-match	Изменяет порядок выбора для поиска несовпадающих строк.
-w, --word-regexp	Выбирает только строки, содержащие совпадения, которые образуют целые слова.
-x, --line-regexp	Выбирает только те совпадения, которые полностью соответствуют всей строке.
-c, --count	Скрывает обычный вывод, вместо этого выводит количество совпадающих строк, с опцией "-v, --invert-match" - количество несовпадающих строк.
-m NUM, --max- count=NUM	Завершает поиск после нахождения указанного количества "NUM" строк.
-n, --line-number	Индексирует все строки стандартного вывода команды (command) номерами, начиная с 1.
-A NUM, --after- context=NUM	Выводит заданное количество "NUM" строк, расположенных после "A" строк, содержащих заданный шаблон. Результирующий вывод для более комфортного представления разделен на группы с помощью знаков (--).
-B NUM, --before- context=NUM	Выводит заданное количество "NUM" строк, расположенных до "B" строк, содержащих заданный шаблон. Результирующий вывод для более комфортного представления разделен на группы с помощью знаков (--).
-C NUM, -- context=NUM	Выводит заданное количество "NUM" строк, расположенных до и после "C" строк, содержащих заданный шаблон. Результирующий вывод для более комфортного представления разделен на группы с помощью знаков (--).

gps

Команда управления приемником GPS/ГЛОНАСС.

Синтаксис:

#1> gps [options] [command]

Options:

```
-t=<level> - turn trace level (1, 2 or 0 - turn trace off)
-i=<int>    - set integrator time constant in seconds
-a[=(0:1)] - turn the power on the antenna amplifier
-r[=(0:1)] - set reset signal
-p=<port>   - set TCP port for service (2323 by default)
-s=<baudrate|0> - set baud rate for GPS NMEA port (0 - set 115200)
```

Command:

```
start      - start GPS service
stop       - stop  GPS service
coordinates - show  GPS coordinates
console    - map  GPS NMEA port to stdin/stdout
tcp        - map  GPS NMEA port to TCP service
stat       - show GPS statistics
clear      - clear GPS statistics
```

Параметр	Описание
-t=<level>	Уровень вывода в системный журнал служебных сообщений: • "2" – запись в системный журнал всех NMEA-сообщений, полученных от приемника GPS/ГЛОНАСС. • "1" – запись в системный журнал только сообщений об обнаружении/потере приемника GPS/ГЛОНАСС, об изменении количества видимых спутников или о существенном изменении координат и т.п. • "0" – сообщения не записываются, трассировка отключена.
-a[=(0:1)]	Включение/отключение подачи питания на антенный усилитель (при его наличии): • "1" – включить питание (по умолчанию, если значение не задано). • "2" – отключить питание.
start	Запуск службы GPS.
stop	Остановка работы службы GPS.
coordinates	

Просмотр информации о текущем состоянии приемника GPS/ГЛОНАСС и статистике его работы.

Пример вывода команды:

```
#1> gps coordinates
Satellites: 8
LAT/LONG:   56.811911/60.547041
Altitude:   275.89
HDOP:       0.92
FIX:        3D, GLONASS
Total GPS time: 17:43:19
Total nonvalid time: 00:00:01(0%)
Number of losses: 0
Now coordinates are valid last 17:43:18
Satellites histogram:
    ^
    |
2.0 +
    |
3.0 +
    |
4.0 +
    |
5.0 +
    | <1%
6.0 +
    | 1%
7.0 +
      ||||||||||||||||||||| 99%
    v
SATmin= 5 SATmax= 10
```

- "Satellites" – текущее количество видимых спутников.
- "LAT/LONG" – географические координаты приемника в градусах:
 - "LAT (*latitude*)" – широта от -90.0000000° до +90.0000000°.
 - "LONG (*longitude*)" – долгота от -180.0000000° до +180.000000°.
- "Altitude" – высота над уровнем моря в метрах.
- "HDOP" – коэффициент снижения точности координат в горизонтальной плоскости.



ПРЕДОСТЕРЕЖЕНИЕ

Для надежной временной синхронизации рекомендуется использовать значения параметра "HDOP" не более 1.5.

Система (используемая ГНСС) может принимать значения:

- GPS.
- GLONASS.
- GPS+GLONASS.

Далее приводятся статистические данные (могут быть получены отдельно с помощью команды `"gps stat"`):

- "Total GPS time" – полное время работы службы GPS с момента ее запуска командой "gps start".
- "Total nonvalid time" – время, в течение которого координаты были неизвестны.
- "Number of losses" – количество случаев потери координат.
- "Now coordinates are valid last ..." – время работы службы GPS с момента последнего обнаружения координат.
- "Satellites histogram" – гистограмма количества видимых спутников.
- "SATmin" и "SATmax" – минимальное и максимальное количество видимых спутников соответственно, зафиксированное с момента последнего сброса статистики.
- "FIX - NO FIX|2D|3D, <unknown>|GPS|GLONASS|GPS+GLONASS" – текущее состояние захвата (определения) координат. Отображает значения в виде "текущий режим определения координат", <система>. Текущий режим определения координат может принимать значения:

	• "NO FIX" – координаты не определены. • "2D" – определены широта и долгота. • "3D" – определены широта, долгота и высота над уровнем моря.
stat	Просмотр статистических данных о работе приемника GPS/ГЛОНАСС (без информации о текущем состоянии приемника).
clear	Сброс статистических данных.

**ПРЕДОСТЕРЕЖЕНИЕ**

Обратите внимание, что команды "tcp", "console" и параметры "-i", "-r", "-p" и "-s" используются для диагностики и отладки в экстренных случаях и только специалистами.

**ВНИМАНИЕ**

Команда "gps" доступна только в версии программного обеспечения с поддержкой технологии TDMA.

tsync

Команда вывода статистики синхронизации времени от внутреннего приемника ГНСС.

Синтаксис:

```
tsync [command]
Command:
  enable [BAUDRATE] - enable external synchronization sources
  disable           - disable external synchronization sources
  [no]trace         - turn trace (debug) messages output to syslog
  [show]            - show statistics
  clear             - clear statistics
```

Параметр	Описание
enable [BAUDRATE]	Включение внешнего источника синхронизации.
disable	Отключение внешнего источника синхронизации.
[no]trace	Включение трассировки (отладки) вывода сообщений в системный журнал.
[show]	Вывод статистики.
clear	Сброс статистики.

**ВНИМАНИЕ**

Команда "tsync" доступна только в версии программного обеспечения с поддержкой технологии TDMA.

Протокол SSH

Протокол SSH (Secure Shell) обеспечивает безопасное удаленное управление сетевыми устройствами. Его функциональность аналогична протоколу Telnet, но, в отличие от Telnet, SSH кодирует все протокольные сообщения, включая передаваемые пароли. Протокол SSH использует клиент-серверную архитектуру. Сервер SSH принимает соединения от клиентов SSH, выполняет их авторизацию и предоставляет доступ к командной оболочке.

Все устройства "Инфинет" имеют встроенные функции сервера и клиента SSH.

sshd

Настройка встроенного сервера SSH (SSH-демона) выполняется с помощью команды "*sshd*". По умолчанию сервер SSH отключен.

Доступ к устройству по протоколу SSH может быть ограничен с помощью списка контроля доступа "*\$ACLOCAL*". Когда на устройстве настроен список контроля доступа, сервер SSH отклоняет все попытки подключения от клиентов SSH с IP-адресом, которого нет в списке.

Синтаксис:

```
sshd -help, -h
sshd -port=PORT
sshd -window=SIZE
sshd -keepalive=TIME
sshd -banner=on | off
sshd -log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL} [notice]
sshd -algo-list
sshd -kex-algos[=ALGO-LIST]
sshd -hostkey-algos[=ALGO-LIST]
sshd -cipher-algos[=ALGO-LIST]
sshd -hash-algos[=ALGO-LIST]
sshd -comp-algos[=ALGO-LIST]
sshd -auth-methods[=AUTH-METHODS-LIST]
sshd -none-cipher=on | off
sshd start
sshd stop
sshd newkeys
sshd pub[key] {sh[ow] | cl[ear] | de[lete] N}
sshd pub[key] {in[stall] | im[port] [LOGIN[:PASSWORD]@]HOST/FILE} [COMMENT]
sshd tun[nel] add LOGIN PASSWORD IFNAME
sshd tun[nel] del LOGIN | clear
```

Параметр	Описание
-help, -h	Вывод синтаксиса команды " <i>sshd</i> ".
-port=PORT	Номер порта TCP, на котором сервер SSH должен принимать подключения, по умолчанию 22.
-window=SIZE	Размер внутреннего окна приема сервера SSH, указывается в байтах. Размер окна сервера SSH определяет максимально допустимую пропускную способность для канала данных " <i>SSH Client - SSH Server</i> ". По умолчанию размер окна составляет 24576 байт.
-keepalive=TIME	Установка периода продолжительности проверки активности сеанса в секундах. По умолчанию сервер не выполняет проверку активности, значение 0.
-banner=on off	Показывать/скрывать информационный баннер ОС WANFlex пользователю после прохождения авторизации.
-log-level={emerg alert crit error warning notice info debug LEVEL} [notice]	Уровень журналирования, определяющий детализацию регистрируемых в системном журнале сообщений сервера SSH. Для управления системным журналом используйте команду " <i>sys log</i> ". Различные уровни журналирования определяются аргументами " <i>emerg</i> ", " <i>alert</i> ", " <i>error</i> ", " <i>warning</i> ", " <i>notice</i> ", " <i>info</i> ", " <i>debug</i> ", либо могут устанавливаться номером необходимого уровня (от 0 до 7) с использованием числового аргумента " <i>LEVEL</i> ". По умолчанию включен уровень " <i>info</i> " (уровень 6).
-algo-list	Отображение списка всех доступных алгоритмов SSH для обмена ключами (kex), аутентификации (host key), кодирования данных (cipher), проверки данных (hash) и сжатия данных (comp).
-kex-algos[=ALGO-LIST]	Выбор алгоритмов kex из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе обмена ключами SSH.
-hostkey-algos[=ALGO-LIST]	Выбор алгоритма формирования ключа/отпечатка сервера из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе аутентификации "Сервер-Клиент" SSH.
-cipher-algos[=ALGO-LIST]	Выбор алгоритмов кодирования из списка алгоритмов (ALGO-LIST), которые будут использоваться при кодировании данных SSH.
-hash-algos[=ALGO-LIST]	Выбор алгоритма хеширования из списка алгоритмов (ALGO-LIST), которые будут использоваться при проверке данных SSH.
-comp-algos[=ALGO-LIST]	Выбор алгоритма сжатия из списка алгоритмов (ALGO-LIST), которые будут использоваться при сжатии данных SSH.

-auth-methods[=AUTH-METHODS-LIST]	Выбор доступного метода аутентификации из списка (AUTH-METHODS-LIST). Значение "all" включает все методы аутентификации.
-none-cipher=on off	Включение/отключение использования кодирования. Используется в тех случаях, когда нужен простой туннель TCP, что существенно уменьшает нагрузку на процессор.
start	Запуск сервера SSH.
stop	Останов сервера SSH.
newkeys	Повторное создание ключей сервера.  ВНИМАНИЕ При первом запуске сервер SSH генерирует ключи DSS и RSA, которые будут использоваться для аутентификации с использованием публичного ключа.
pub[key] {sh[ow] cl[ear] de[lete] N}	• "show" – вывод информации о публичных ключах клиентов SSH, зарегистрированных в реестре сервера SSH. • "clear" – удаление всех публичных ключей клиентов SSH из реестра. • "delete" – удаление публичных ключей клиента SSH из реестра сервера SSH. Параметр "N" – индекс ключа в списке.
pub[key] {in[stall] im[port] [LOGIN::PASSWORD]@]HOST /FILE} [COMMENT]	Активация аутентификации клиентов SSH с помощью публичного ключа. В этом режиме сервер SSH разрешает клиенту SSH использовать ключ вместо ручного ввода пароля. Этот режим включается автоматически, как только открытый ключ клиента SSH будет добавлен в реестр сервера SSH: • "install" – установка публичного ключа клиента SSH в реестр сервера SSH. • "import" – импорт публичного ключа клиента SSH в реестр сервера SSH с удаленного сервера FTP: • "HOST" – IP-адрес удаленного сервера FTP. • "FILE" – файл, содержащий публичный ключ клиента RSA/DSS в формате OpenSSH или SSH2. Если удаленный сервер FTP требует аутентификацию, то имя пользователя и пароль должны быть указаны в "LOGIN" и "PASSWORD" соответственно. • "COMMENT" – данный аргумент позволяет добавить комментарий к записи публичного ключа в реестре. По умолчанию добавляется комментарий с IP-адресом клиента или IP-адресом сервера FTP, из которого получен ключ.
tun[nel] add LOGIN PASSWORD IFNAME	Установка отдельных параметров аутентификации для каждого интерфейса tap: • "LOGIN" – имя пользователя. • "PASSWORD" – пароль. • "IFNAME" – имя интерфейса tap. Если указанные аргументы не определены, то будут использоваться общесистемные параметры доступа.
tun[nel] del LOGIN clear	• "del LOGIN" – удалить указанное имя пользователя из конфигурации SSH Tunnel. • "clear" – удалить всех пользователей SSH Tunnel из конфигурации сервера SSH.

**ВНИМАНИЕ**

По умолчанию сервер SSH применяет только парольную аутентификацию. Однако этого может оказаться недостаточно для обеспечения необходимого уровня безопасности. У устройств "Инфинет" есть несколько встроенных методов аутентификации SSH, которые управляются командами "sshd pubkey" и "sshd -auth-methods". При этом сервер SSH сохранит открытый ключ подключенного клиента SSH.

sshc

Настройка встроенного клиента SSH выполняется с помощью команды "sshc".

Синтаксис:

```
sshc [options] [LOGIN@]HOST[:PORT] [REMOTE-COMMAND]
options:
  -help, -h
  -window=SIZE
  -keepalive=TIME
  -compress, -C
  -bind-addr=ADDR, -b ADDR
  -pubkey-show
  -pubkey-new[=BITS]
  -pubkey-clear
  -pubkey-export=[LOGIN[:PASSWORD]@]HOST/FILE
  -algo-list
  -kex-algos[=ALGO-LIST]
  -hostkey-algos[=ALGO-LIST]
  -cipher-algos[=ALGO-LIST], -c ALGO-LIST
  -hash-algos[=ALGO-LIST], -m ALGO-LIST
  -comp-algos[=ALGO-LIST]
```

Параметр	Описание
[options] [LOGIN@]HOST: PORT] [REMOTE- COMMAND]	Подключение к удаленному серверу SSH: "<i>LOGIN</i>" – имя пользователя (может быть опущено, если имя учетной записи на удаленном узле совпадает с именем учетной записи, от которой выполняется подключение). "<i>HOST</i>" – IP-адрес удаленного устройства. "<i>REMOTE-COMAND</i>" – команда, которая должна быть выполнена на сервере SSH после успешного входа в систему.
-help, -h	Вывод синтаксиса команды " <i>sshc</i> ".
-window=SIZE	Размер внутреннего окна приема клиента SSH в байтах. Размер окна определяет максимальную пропускную способность для канала данных "SSH Server - SSH Client". По умолчанию размер окна клиента SSH составляет 24576 байт.
-keepalive=TIME	Установка частоты отправки на сервер обязательных подтверждений активности сеанса. Это позволяет не потерять сессию с сервером, когда активность пользователя в рамках текущего подключения отсутствует в течение длительного периода времени. По умолчанию клиент SSH не отправляет никаких специальных подтверждений активности (значение 0). Измеряется в секундах.
-compress, -C	Включение сжатия данных для создаваемого подключения.
-bind-addr=ADDR, -b ADDR	Установка IP-адреса источника пакетов SSH. Указанный IP-адрес заменяет значение в поле IP-адреса отправляемых пакетов SSH.
-pubkey-show	Вывод информации о сформированных публичных ключах.
-pubkey-new [BITS]	Создание новых открытых ключей клиента DSS и RSA. Аргумент "BITS" должен быть указан как размер ключа в битах, возможные значения: 512-4096.
-pubkey-clear	Удаление публичных ключей из реестра клиента SSH.
-pubkey-export=[LOGIN[:PASSWORD]@]HOST/FILE	Экспорт открытых ключей из реестра клиента SSH в файл на удаленном сервере FTP: "<i>HOST</i>" – IP-адрес удаленного сервера FTP. "<i>FILE</i>" – имя файла, которое будет содержать публичные ключи RSA/DSS. Если удаленный сервер FTP требует аутентификацию, то имя пользователя и пароль должны быть указаны в "<i>LOGIN</i>" и "<i>PASSWORD</i>" соответственно.
-algo-list	Список всех доступных алгоритмов SSH для обмена ключами (kex), аутентификации (hostkey), кодирования данных (cipher), проверки данных (hash) и сжатия данных (comp).
-kex-algos [ALGO-LIST]	Выбор алгоритма kex из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе обмена ключами SSH.
-hostkey-algos [ALGO-LIST]	Выбор алгоритма формирования ключа/отпечатка сервера из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе аутентификации сервера-клиента SSH.

-cipher-algos [=ALGO-LIST], -c ALGO-LIST	Выбор алгоритма кодирования из списка алгоритмов (ALGO-LIST), которые будут использоваться при кодировании данных SSH.
-hash-algos [=ALGO-LIST], -m ALGO-LIST	Выбор алгоритма хеширования из списка алгоритмов (ALGO-LIST), которые будут использоваться при проверке данных SSH.
-comp-algos [=ALGO-LIST]	Выбор алгоритма сжатия из списка алгоритмов (ALGO-LIST), которые будут использоваться при сжатии данных SSH.



ВНИМАНИЕ

Для принудительного прерывания сеанса клиента SSH (например, если SSH-сервер не отвечает на запросы SSH-клиента), используйте следующую последовательность клавиш: "Enter~." (На клавиатуре сначала нажмите клавишу "Enter", затем "~", затем ".").

sshtun

Команда "sshtun" позволяет создать до 16 независимых [туннелей](#) L2 через соединения SSH.

Для создания туннелей на обеих сторонах соединения должен быть создан и настроен интерфейс tap командой "ifconfig tapX up". Интерфейс tap может иметь IP-адрес и использоваться как самостоятельный сетевой интерфейс, например, для маршрутизации, а также в составе группы коммутации. Кроме того, интерфейс tap может быть использован в качестве родительского для интерфейсов vlan, lag и prf, в том числе для использования в составе сети MINT.

Клиентский модуль SSH Tunnel автоматически переустанавливает соединение с удалённым сервером при перезагрузке устройства или разрыве связи. Может работать за NAT, в том числе с адресами, получаемыми динамически по протоколу DHCP.

Синтаксис:

```
sshtun -help, -h
sshtun -log-level={emerg|alert|crit|error|warning|notice|info|debug|LEVEL}
sshtun -algo-list
sshtun start | stop | clear
sshtun IFNAME [options] [LOGIN[:PASSWORD]@HOST[:PORT]] [start | stop | del[ete]]
options:
  -window=SIZE
  -keepalive=TIME
  -compress=on | off, -C on | off
  -bind-addr=ADDR, -b ADDR
  -remote-if=REMOTE_TAP_NUM
  -reconnect-delay=TIME
  -kex-algos[=ALGO-LIST]
  -hostkey-algos[=ALGO-LIST]
  -cipher-algos[=ALGO-LIST], -c ALGO-LIST
  -hash-algos[=ALGO-LIST], -m ALGO-LIST
  -comp-algos[=ALGO-LIST]
  -auth-methods[=AUTH-METHODS-LIST]
  -none-cipher=on | off
```

Параметр	Описание
-help, -h	Вывод синтаксиса команды "sshtun".
-log-level={emerg alert crit error warning notice info debug LEVEL}	Уровень журналирования, определяющий детализацию регистрируемых в системном журнале сообщений сервера SSH. Для управления системным журналом используйте команду "sys log". Различные уровни журналирования определяются аргументами "emerg", "alert", "error", "warning", "notice", "info", "debug", либо могут устанавливаться номером необходимого уровня (от 0 до 7) с использованием числового аргумента "LEVEL". По умолчанию включен уровень "info" (уровень 6).

-algo-list	Отображение списка всех доступных алгоритмов SSH для обмена ключами (kex), аутентификации (host key), кодирования данных (cipher), проверки данных (hash) и сжатия данных (comp).
start stop clear	Запуск / останов / очистка конфигурации SSH Tunnel.
IFNAME [options] [LOGIN [:PASSWORD]@HOST[:PORT]] [start stop del [ete]]	Запуск / останов / удаление из конфигурации данного экземпляра туннеля SSH. Параметры для установления туннеля SSH: • "IFNAME" – имя интерфейса tap удаленного сервера SSH. • "LOGIN" – имя пользователя удаленного сервера SSH. • "PASSWORD" – пароль удаленного сервера SSH. • "HOST" – IP-адрес удаленного сервера SSH. • "PORT" – номер порта удаленного сервера SSH.
-window=SIZE	Размер внутреннего окна приема клиента SSH в байтах. Размер окна определяет максимальную пропускную способность для канала данных "SSH Server - SSH Client". По умолчанию размер окна клиента SSH составляет 24576 байт.  ВНИМАНИЕ Для достижения максимальной производительности, параметр "-window" на обоих сторонах туннеля следует устанавливать в значения не менее 128000.
-keepalive=TIME	Установка частоты отправки на сервер обязательных подтверждений активности сеанса. Это позволяет не потерять сессию с сервером, когда активность в рамках текущего подключения отсутствует в течение длительного периода времени. По умолчанию клиент SSH не отправляет никаких специальных подтверждений активности (значение 0). Измеряется в секундах.
-compress=on off, -Con off	Включение сжатия данных для создаваемого туннеля.
-bind-addr=ADDR, -b ADDR	Установка IP-адреса источника пакетов SSH. Указанный IP-адрес заменяет значение в поле IP-адреса отправляемых пакетов SSH.
-remote-if=REMOTE_TAP_NUM	Номер интерфейса tap на удалённой стороне.
-reconnect-delay=TIME	Таймаут для повторной попытки установления соединения при разрыве связи.
-kex-algos[=ALGO-LIST]	Выбор алгоритмов kex из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе обмена ключами SSH.
-hostkey-algos[=ALGO-LIST]	Выбор алгоритма формирования ключа/отпечатка сервера из списка алгоритмов (ALGO-LIST), которые будут использоваться в процессе аутентификации сервера-клиента SSH.
-cipher-algos[=ALGO-LIST], -c ALGO-LIST	Выбор алгоритма кодирования из списка алгоритмов (ALGO-LIST), которые будут использоваться при кодировании данных SSH.
-hash-algos[=ALGO-LIST], -m ALGO-LIST	Выбор алгоритмов хеширования из списка алгоритмов (ALGO-LIST), которые будут использоваться при проверке данных SSH.
-comp-algos[=ALGO-LIST]	Выбор алгоритмов сжатия из списка алгоритмов (ALGO-LIST), которые будут использоваться при сжатии данных SSH.
-auth-methods[=AUTH-METHODS-LIST]	Список доступных методов проверки подлинности.
-none-cipher=on off	Включение/отключение использования кодирования. Используется в тех случаях, когда нужен простой туннель TCP, что существенно уменьшает нагрузку на процессор.

nslookup

Утилита Nslookup отправляет запросы к серверу DNS для прямого и обратного преобразования доменных имен.

Синтаксис:

```
nslookup {name|ip}
```

Параметр	Описание
<i>name</i>	Формирует запрос по доменному имени для получения IP-адреса.
<i>ip</i>	Формирует запрос по IP-адресу для получения доменного имени.

DNSclient

Клиент DNS – модуль, обеспечивающий определение адреса узла по его полному имени.

Синтаксис:

```
dnsclient [options] [command]
where commands are:
  start - start service
  stop  - stop service
where options are:
  -domain={name}    - set local domain name.
  -server={address} - set Internet address (in dot notation) of a name server,
                      this option can be repeated.
```

Параметр	Описание
<i>start</i>	Запуск службы DNS-клиент.
<i>stop</i>	Остановка службы DNS-клиент.
<i>-domain={name}</i>	Установка локального имени домена.
<i>-server={address}</i>	Установка адреса сервера. Данный параметр может быть задан несколько раз.

Параметр	Описание
----------	----------

get	Загрузка на устройство новой версии программного обеспечения. Загрузка выполняется по протоколу FTP. В качестве имени файла следует указать полное имя в формате используемой файловой системы. Процесс загрузки делится на две фазы: • Считывание файла с удалённого сервера и проверка его целостности. • Запись образа системы в память маршрутизатора. Вторая фаза отображается на экране повторяющимся знаком ".". Для обновления с официального ftp-сервера компании "Инфинет", используйте команду: <pre>flashnet get ftp:ftp@ftp://92.168.100.34/firmware.H11S01v1.6.6.bin</pre> где • "H11" – аппаратная платформа. • "1.6.6" – версия программного обеспечения. • "ftp" – имя пользователя. • "ftp" – пароль.  ВНИМАНИЕ После установки нового программного обеспечения, устройство необходимо перезагрузить командой: <pre>restart yes</pre>
put	Выгрузка программного обеспечения на внешний сервер.
-S	С помощью этой опции можно подставить любой другой IP-адрес.

cron

ОС WANFleX позволяет настроить выполнение некоторых команд в заданное время или с определённой периодичностью. Таким образом, например, можно выполнять регулярное резервное копирование конфигурации без участия системного администратора.

Синтаксис:

```
cron start
cron stop
cron clear
cron add commandID "command" [from][-to][\interval]
cron del commandID
cron dump
```

Examples from or to:
 31/12/2016 12:00:00
 31/12/2016 12:00
 12:00:00
 12:00

Any field can be set as '.' - don't care.

Examples of intervals

```
DD HH:MM:SS
\ 2 12:33:15
\ 2 12:33
\ 12:33:15
\ 12:33
\ 2
```

Don't care not allowed.

Параметр	Описание
start	Запуск службы Cron.
stop	Останов службы Cron.
clear	Удаление всех записей таблицы.
add commandID "command" [from [-to][interval]	Добавляет новую запись в таблицу Cron: "commandID" – произвольное название записи. "command" – команда к выполнению. "from" и "-to" – позволяют настроить точные дату и/или время выполнения команды. Допустимые форматы (любой символ может быть заменён на ".", если допустимы любые значения): 31/12/2016 12:00:00 31/12/2016 12:00 12:00:00 12:00 "interval" – позволяют настроить периодичность выполнения команды. Допустимые форматы (символ "." недопустим): \ 2 12:33:15 \ 2 12:33 \ 12:33:15 \ 12:33 \ 2  ВНИМАНИЕ Команды, в которых указаны точная дата и/или время будут работать только если дата и время в системе синхронизированы по sntp или gps. В противном случае, исполняться будут только команды, в которых указан период выполнения, например, каждые 7 дней (с момента перезагрузки устройства).
del commandID	Удаляет запись из таблицы Cron.
dump	Просмотр таблицы

Пример:

Настроим выполнение резервного копирования конфигурации каждые 6 дней.

```
#1> cron add TEST "co export test:admin@11.12.13.14/testserver/1111" \6
cron: ID 'TEST' replaced
#1> cron start
#1> cron dump
id='TEST' range=' \ 6' command='co export test:admin@11.12.13.14/testserver/1111' next='23/07/2019 10:40:29'
```