D-Link®

DSA-3110

Концентратор доступа

Руководство по использованию
интерфейса командной строки

Rev. 0.06 (Aug 2007)

RECYCLABLE

Содержание

Описание устройства

DSA-3110 представляет собой концентратор доступа для подключения пользователей к удаленной сети через VPN по протоколам PPTP и PPPoE. Устройство обеспечивает подключение и авторизацию пользователей, а также выдачу статистики по подключениям на внешний сервер с использованием технологии NetFlow. DSA-3110 предоставляет законченное решение обеспечивающее подключение клиентов к Интернет внутри сетей провайдеров с выдачей статистики по израсходованному трафику на сервер хранения или биллинга, а также подключение мобильных сотрудников к внутренней сети организации по безопасному VPN-соединению с возможностью учета производимых подключившимися пользователями действий.

DSA-3110 совместим с большинством популярных операционных систем, включая Macintosh, *BSD, UNIX, Linux и Windows, и может быть интегрирован в крупную сеть.

Характеристики DSA-3110

Аппаратные характеристики:

- Процессор: Intel Xscale 533MHz
- 64MB RAM
- 16 MB Flash ROM
- 7 портов 10/100Base-TX
- 4 независимо конфигурируемых интерфейса 10/100Base-TX
- Внешний блок питания 5В 3А
- Светодиодные индикаторы питания и состояния подключений к интерфейсам
- Консольный порт RS-232

Программное обеспечение:

- Базовая операционная система: Linux
- Сервер PPTP
- Экспорт статистики по протоколу NetFlow
- NAT
- Статическая маршрутизация
- Внешний syslog-сервер
- Авторизация VPN-подключений: локально или RADIUS
- Поддержка до 250 пользователей в локальной базе
- Поддержка до 50 одновременных подключений
- WEB-интерфейс управления с двухязыковой поддержкой (русский и английский)
- SSH-сервер
- Интерфейс командной строки CLI
- Telnet сервис (по умолчению отключен)
- Конфигурация интерфейсов со статическим адресом или DHCP
- Многочисленные возможности iptables, ip, tc и других утилит, доступные для настройки через стандартную командную строку встроенного Linux

Установка

DSA-3110 предоставляет средства конфигурирования на основе безопасного клиента Secure Shell (SSH), Telnet и консольного доступа.

Примечание: По умолчанию в целях безопасности telnet сервис на устройстве отключен. Для его активации прочтите раздел **Включение и выключение автозагрузки сервисов** данного руководства.

Включение DSA-3110.Начало работы с устройством.

Перед тем, как начать настройку концентратора доступа, необходимо установить с ним физическое соединение. Для этого потребуется:

1. Компьютер с ОС Linux, *BSD, UNIX, Windows или MacOS
2. Клиент SSH (secure shell) или Telnet для доступа через сеть, эмулятор терминала для доступа к консоли
3. Кабели Ethernet для подключения к сети (RJ-45) или консольный кабель RS-232 (поставляется в комплекте) для работы с консолью.

Далее:

1. Подключите один конец кабеля RJ-45 к любому из портов встроенного коммутатора (порты 4-7), а другой конец к доступному порту Ethernet компьютера или коммутатора существующей локальной сети.
2. Подключите адаптер питания, входящий в комплект поставки к устройству и к сети питания 220В.

Подключение к DSA-3110 через порт RS-232 .

Для того чтобы подключиться порту RS-232 управления устройства, на рабочей станции необходимо:

- подключить консольный кабель, входящий в комплект устройства, к свободному COM-порту рабочей станции одним концом и к порту RS-232 устройства DSA-3110 другим концом.
- запустить HyperTerminal или иную терминальную программу, с со следующими параметрами соединения (Port Settings):

  Скорость порта (Bit per second) –115200
  Количество бит данных (Data Bits)-8
  Контроль четности (Parity) – None
  Количество стоп-бит (Stop Bits) - 1
  Контроль потока (Flow Control) - None

По умолчанию для авторизации в консольном режиме установлены следующие имя пользователя и пароль: имя пользователя (**User name) - root**, пароль (**Password) - admin**.

Внутренняя структура программного обеспечения устройства реализована максимально приближенно к настольным системам Linux. Пользователи могут изменять любые конфигурационные файлы используемых служб, создавать новые, включать и выключать автозагрузку.

После изменения конфигурации ее необходимо сохранять командой **saveconfig** -- данная команда сохраняет содержимое конфигурационного каталога /etc в энергонезависимой памяти. При изменении конфигурации следует помнить, что сохраняются ТОЛЬКО изменения, сделанные в каталоге /etc.

Для редактирования конфигурации непосредственно на устройстве можно использовать встроенный редактор vi или nano.

Внимание: файл hwmanag, присутствующий в прошивке устройства, предназначен для специализированных инженерных целей компании D-link. Не пытайтесь изменять его или работать с ним через консольный режим. Это может привести к неработоспособности

устройства.

Настройка устройства с помощью интерфейса командной строки

Настройка сетевых интерфейсов

Порты eth-0 –eth-3 имеют следующую привязку к цифровым обозначениям портов, нанесенных на корпус устройства:
Eth-0 – порты 4 -7
Eth-1 – порт 3
Eth-2 - порт 1
Eht-3 - порт 2

Порты 4-7 - представляют собой коммутатор с изолированными портами (т.е. передача пакетов между портами коммутатора запрещена, только на другие интерфейсы.

По умолчанию на устройстве создан 1 интерфейс Ethernet со статическим IP адресом:
Eth-0 - 192.168.1.254

Конфигурационный файл настройки интерфейсов располагается в каталоге /etc/network и называется interfaces. Данный файл имеет несколько секций, отвечающих за конфигурацию определенных параметров.

- **секция *auto*: интерфейсы для автоматического запуска при загрузке.**

  Формат: auto <список интерфейсов>

  Пример использования: auto lo eth0

  Пояснения к примеру: сконфигурированы для автоматического запуска интерфейсы lo (loopback) и eth0 (первый Ethernet-интерфейс)

- **секция *iface*: конфигурация интерфейса**

  Формат: iface <имя интерфейса> inet <тип интерфейса>

  Пример использования: iface eth0 inet dhcp

  Пояснения к примеру: интерфейс eth0 конфигурируется с использованием DHCP

- тип **static** - статический IP-адрес
  - параметр **address –** задание адреса интерфейса

    Формат: **address <ip-адрес>**

    Пример использования: address 192.168.1.254

    Пояснения к примеру: интерфейсу присвоен адрес 192.168.1.254

    Обязательный параметр.
  - параметр **netmask –** задание сетевой маски

    Формат: **netmask <маска подсети>**

    Пример использования: **netmask 255.255.255.0**

    Пояснения к примеру: интерфейсу присвоена сетевая маска 255.255.255.0

    Обязательный параметр.
  - параметр **gateway –** адрес шлюза по умолчанию

    Формат: **gateway <ip-адрес>**

    Пример использования: **gateway 192.168.1.1**

    Пояснения к примеру: назначен маршрут по умолчанию через маршрутизатор с адресом 192.168.1.1

- параметр **metric –** установка приоритета интерфейса для маршрутизации

  Формат: **metric <метрика>**

  Пример использования: **metric 50**

  Пояснения к примеру: приоритет интерфейса понижен до уровня 50
- параметр **hwaddr –** присвоение MAC-адреса

  Формат: **hwaddr <mac-адрес>**

  Пример использования: **hwaddr 00:01:02:03:04:05**

  Пояснения к примеру: интерфейсу назначен MAC-адрес 00:01:02:03:04:05

- тип **dhcp** -- динамическое получение адреса
  - параметр **hwaddr –** присвоение MAC-адреса

    Формат: **hwaddr <mac-адрес>**

    Пример использования: **hwaddr 00:01:02:03:04:05**

    Пояснения к примеру: интерфейсу назначен MAC-адрес 00:01:02:03:04:05

Служба PPP

Конфигурация службы PPP разбита на четыре конфигурационных файла (два для PPTP сервера и два для PPPoE сервера):

1. /etc/pptpd.conf – конфигурация непосредственно сервера PPTP
2. /etc/ppp/options.pptpd – конфигурация протокола PPP, работающего в рамках PPTP-сессии.

3. /etc/default/pppoe-server- конфигурация непосредственно сервера PPPoE
4. /etc/ ppp/pppoe-server-options - конфигурация протокола PPP, работающего в рамках PPPoE-сессии.

Конфигурационный файл /etc/pptpd.conf:

- параметр **remoteip --** пул адресов для выдачи подключающимся клиентам

  Формат: **remoteip <список IP-адресов или сетей>**

  Пример использования: **remoteip 192.168.1.20-40,192.168.2.12**

  Пояснения к примеру: для выдачи подключающимся клиентам выделены адреса с 192.168.1.20 по 192.168.1.40 и 192.168.2.12

  Примечание: каждый подключившийся клиент использует 1 уникальный адрес из выделенных этим параметром.
- параметр **localip** – пул адресов сервера

  Формат: **localip <список IP-адресов или сетей>**

  Пример использования: **localip 192.168.1.120-140,192.168.2.11**

  Пояснения к примеру: для использования сервером выделены адреса с 192.168.1.120 по 192.168.1.140 и 192.168.2.11

  Примечание: данный адрес используется со стороны сервера, может быть одинаковым для всех подключений

Конфигурационный файл /etc/default/pppoe-server

- параметр **iface –** физический ethernet интерфейса(ов), на котором запускает pppoe сервер
- параметр **cname –** Имя концентратора (Access concentrator name).Служит для разделения сервисов, когда в сети присутствуют несколько серверов PPPoE.

- параметр **sname-** Имя сервиса (Service name).Служит для разделения сервисов,когда в сети присутсвуют несколько серверов PPPoE
- параметр **remoteip --** пул адресов для выдачи подключающимся клиентам

  Формат: **remoteip <список IP-адресов или сетей>**

  Пример использования: **remoteip 192.168.1.20-40,192.168.2.12**

  Пояснения к примеру: для выдачи подключающимся клиентам выделены адреса с 192.168.1.20 по 192.168.1.40 и 192.168.2.12

  Примечание: каждый подключившийся клиент использует 1 уникальный адрес из выделенных этим параметром.
- параметр **localip** – адрес сервера

  Формат: **localip <список IP-адресов или сетей>**

  Пример использования: **localip 192.168.1.120**

  Примечание: Разрешает использовать только один local ip адрес (пул невозможен).Данный адрес используется со стороны сервера, и одинаков для всех подключений

Конфигурационный файл /etc/ppp/options.pptpd

- параметры **refuse-<протокол>, require-<протокол>, где протокол -- pap, chap, mschap, mschapv2 -** используемые протоколы авторизации

  Префикс refuse используется для запрещения авторизации по данному протоколу, префикс require – для принудительного выбора протокола.

  Формат: **refuse-<протокол>**

  require-<протокол>

  Пример использования: **refuse-pap**

  Пояснения к примеру: протокол аутентификации PAP запрещен
- параметр **refuse-mppe,** параметр **require-mppe –** шифрование

  Формат: **refuse-mppe**

  require-mppe

  Пример использования: **require-mppe**

  Пояснения к примеру: включено обязательное шифрование подключений
- параметр **plugin –** подключение дополнительных модулей PPP

  Используется для переключения механизма авторизации пользователей на внешний RADIUS-сервер.

  Формат: **plugin radius.so**

  plugin radattr.so

  Пример использования: **plugin radius.so**

  plugin radattr.so

  Пояснения к примеру: авторизация пользователей переключена на внешний сервер RADUIS

За более подробным описанием конфигурационных файлов обращайтесь к справочному руководству по пакетов poptop и rp-pppoe ОС Linux (http://poptop.sf.net)

Конфигурационный файл /etc/ppp/pppoe-server-option

Формат файла совпадает с форматом **/etc/ppp/options.pptpd**

Настройка сервера сбора статистики

Экспортер статистики запускается автоматически после авторизации подключения сценарием /etc/ppp/ip-up.d/1fprobe. Данный сценарий содержит командную строку запуска экспортера fprobe.

- Отключение экспортера:
  снять разрешение на исполнение с файла запуска экспортера командой
  chmod -x /etc/ppp/ip-up.d/1fprobe
- Включение экспортера:
  установить разрешение на исполнение на файл запуска экспортера командой
  chmod +x /etc/ppp/ip-up.d/1fprobe
- Изменение адреса и/или порта сервера сбора статистики:
  адрес указывается последним параметром в командной строке запуска экспортера.

  Формат: **/usr/sbin/fprobe -i $PPP_IFACE <IP-адрес>:<порт>**

  Пример использования: **/usr/sbin/fprobe -i $PPP_IFACE 192.168.100.1:2233**

  Пояснения к примеру: данные статистики будут отправляться на коллектор, находящийся на IP 192.168.100.1 на порту 2233

Настройка шейпинга.

Шейпер позволяет задавать максимальную полосу пропускания для входящих соединений ppp.

Шейпер в DSA-3110 реализован с использованием дисциплины очередей TBF (Token Bucket Filter) и включается автоматически после авторизации подключения сценарием /etc/ppp/ip-up.d/2shaper. Данный сценарий содержит командную строку запуска шейпера.

В настройках по умолчанию данный сценарий отключен.

- Отключение шейпера :
  снять разрешение на исполнение с файла запуска шейпера командой
  chmod -x /etc/ppp/ip-up.d/2shaper
- Включение шейпера:
  установить разрешение на исполнение на файл запуска шейпера командой
  chmod +x /etc/ppp/ip-up.d/2shaper
- Изменение полосы пропускания пакетов шейпера через текстовый редактор vi:

  1. Войти в редактор **vi /etc/ppp/ip-up.d/2shaper**
  2. Нажать **Insert** – вход в режим редактирования
  3. Изменить значение **maxrate** в строке запуска сценария на свое значение:

     tc qdisc add dev $PPP_IFACE root tbf rate maxrate latency 50ms burst 1540

     Параметры запуска, представленные числами являются оптимальными по умолчанию, и их не следует менять без особой необходимости. Подробнее про другие параметры запуска шейпера читайте здесь: http://www.lartc.org

     Пример: **tc qdisc add dev $PPP_IFACE root tbf rate 64kbit latency 50ms burst 1540**

     Пояснения к примеру: данные, поступающие на ppp интерфейс будут искусственно ограничиваться скоростью 64кбит/с.

     Внимание: Измененное значение будет применяться только к следующему **новому** ppp соединению. Для изменения параметров текущих (уже работающих соединений) необходимо их переподключение.

4. Нажать **Escape** для выхода из режима редактирования.
5. Нажать **:wq** для выхода с записью изменений (или **:q!** для выхода без записи).

Ведение журнала событий (syslog)

Конфигурационный файл /etc/default/syslog.

- параметр **SYSLOGD_OPTIONS** – дополнительные ключи запуска демона syslogd

  Формат: **SYSLOGD_OPTIONS="<список дополнительных ключей>"**

  Пример использования: **SYSLOGD_OPTIONS="-S"**

  Пояснения к примеру: демон syslogd будет запущен с ключом -S, уменьшающим количество информации, поступающей в журнал
- параметр **KLOGD_OPTIONS** – дополнительные ключи запуска демона klogd

  Формат: **KLOGD_OPTIONS="<список дополнительных ключей>"**

  Пример использования: **KLOGD_OPTIONS=""**

  Пояснения к примеру: демон klogd будет запущен без дополнительных ключей
- параметр **SYSLOGD_REMOTE** – адрес внешнего сервера сислог.

  Формат: **SYSLOGD_REMOTE="<IP-адрес>[:<порт>]"**

  Пример использования: **SYSLOGD_REMOTE="192.168.1.25"**

  Пояснения к примеру: демон syslogd будет выдавать сообщения на syslog-сервер, расположенный по адресу 192.168.1.25 на стандартный порт (UDP 514).

Настройка трансляции адресов (NAT)

Конфигурационный файл /etc/default/nat

- параметр **NAT_ACTION:** определяет действие для iptables.

  Возможно указание длинной строки действия с дополнительными ключами, например "SNAT --to-source=192.168.1.254". Для выключения трансляции адресов этот параметр должен быть пустым.

  Формат: **NAT_ACTION="<действие>"**

  Пример использования: **NAT_ACTION="MASQUERADE"**

  Пояснения к примеру: для трансляции адресов определяется действие MASQUERADE – трансляция с адреса исходящего интерфейса.
- параметр **NAT_NETS:** определяет сети для трансляции.

  Трансляции будут подвергаться только те пакеты, адреса источника которых принадлежат перечисленным в этом параметре сетям.

  Формат: **NAT_NETS="<список сетей>"**

  Пример использования: **NAT_NETS="192.168.1.0/24 172.20.0.0/16"**

  Пояснения к примеру: для трансляции адресов отбираются только пакеты, приходящие из сетей 192.168.1.0/24 и 172.20.0.0/16.

Включение и выключение автозагрузки сервисов

- **Включение:** в процессе загрузки отрабатываются все ссылки (soft link), находящиеся в каталоге /etc/init.d и начинающиеся с S??, где ?? - порядковый номер для запуска службы. Например S90thttpd - ссылка для запуска службы thttpd, порядковый номер - 90.

Для включения службы в автозапуск необходимо создать ссылку в каталоге /etc/init.d/ на сценарий ее запуска, расположенный в каталоге /etc/init.d/scripts/ командой **ln -s**. Например для включения запуска службы *syslog* необходимо выполнить следующую команду находясь в каталоге /etc/init.d :

ln -s scripts/syslog S45syslog.

При определении номера для запуска следует учитывать, что некоторым службам для нормального функционирования необходима работа других служб. Например, для работы службы Web-сервера (thttpd) требуется поддержка сети (network).

- **Выключение:** для выключения автозагрузки достаточно удалить ссылку удаляемой службы из каталога /etc/init.d

Работа с локальной базой пользователей

Локальная база пользователей состоит из двух независимых баз, содержащих учетные записи пользователей, авторизующихся по протоколу PAP и CHAP соотвественно. Вы можете добавлять, изменять и удалять учетные записи в каждой из баз. База пользователей, авторизующихся по протоколу PAP расположена в файле /etc/ppp/pap-secrets, по протоколу CHAP – /etc/ppp/chap-secrets. Формат обеих баз одинаков и состоит из записей, по одной в каждой строке, имеющих четыре поля.

Формат записи: **user server pass address**

- поле **user:** имя пользователя
- поле **server:** название сервера для подключения или * для любого сервера
- поле **pass:** пароль данного пользователя
- поле **address:** выделяемый пользователю IP-адрес или * для выделения адреса из пула

Пример использования: **user * “password” 192.168.1.22**

Пояснения к примеру: в примере определяется пользователь с именем user, подключающийся к любому серверу, с паролем password. При подключении пользователю выдается IP-адрес 192.168.1.22.

Настройка времени в системе.

Настройка времени в системе производится с помощью программ date и hwclock.
Hwclock используется для сохранения и чтения из памяти аппаратного времени (хранящегося во флеш-памяти устройства по Гринвичу (в формате зоны GMT+0), date используется для установки пользовательского времени с учетом тайм-зоны и перевода на летнее/зимнее время.

Процедура установки времени:

4. Установить тайм-зону, пример:
   export TZ=MSK-3MSD ,где:
   $TZ – переменная, хранящая информацию о тайм-зоне;
   MSK – первое название тайм-зоны (любые три символа);
   -3 –смещение в часах на запад относительно Гринвича (отрицательные числа обозначают зоны GMT+x, положительные GMT-x) ;
   MSD – второе название тайм-зоны. Если оно совпадает с первым, то перевод на летнее/зимнее время осуществляться не будет, если не совпадает хотя бы в одном символе, то перевод осуществляться будет.

2. Установить текущее пользоватльское время (с учетом пояса):
   date MMDDhhmmYYYY, где
   MM-месяц,
   DD-день,
   hh-час,
   mm-минуты,
   YYYY –год.
   Например, date 052614212006 обозначает 26 мая 2006 г. 14:21
5. Сохранить время во флеш памяти устройства.
   hwclock -w

Сохранение конфигурации и сброс к заводским установкам

Для сохранения конфигурации в энергонезависимой памяти используйте команду **saveconfig.**

Для сброса настроек к заводским используйте команду **resetconfig** и перезагрузите устройство.

Для перезагрузки устройства используйте команду **reboot.**