Воскрешение школьного VipNet координатора HW50.

Это дополненная инструкция, которую наш коллега Алексей, получил в Infotecs.

Для работы Координатора у Вас должен быть «свежий» набор DST ключей для доступа в vipnet 2131, который можно получить согласно установленному регламенту.

Глобально обновление состоит из шагов:
1) получение настроек школы из старой конфигурации;
2) перепрошивка координатора на «новый» образ 4.2.4-637;
3) инициализация DST на новой прошивке.

Необходимые условия для обновления координатора:

1) набор DST-ключей
2) вывод команд:

in sh int
in sh ro
in sh dhcp ser

3) прошивка hw50_vipnet_base_i386_4.2.4-637.img

1. Получение набора DST-ключей для доступа к vipnet 2131

Регламент подключения к сети
https://mits.mosreg.ru/upload/iblock/250/rasporyazhenie-ob-utverzhdenii-reglamente-podklyucheniya-k-zashchishchennoy-seti-2131.pdf

При восстановлении DST в нашем случае потребовались фото формуляра с s/n, фото наклейки на координаторе, документ о покупке.

2. Сохранение конфигурации школы

Для сохранения настроек подключения школы и ввода команд в консоли у Вас должен быть пароль пользователя user для доступа консоли. Наш установщик «Калуга Астрал» таких данных не предоставил.

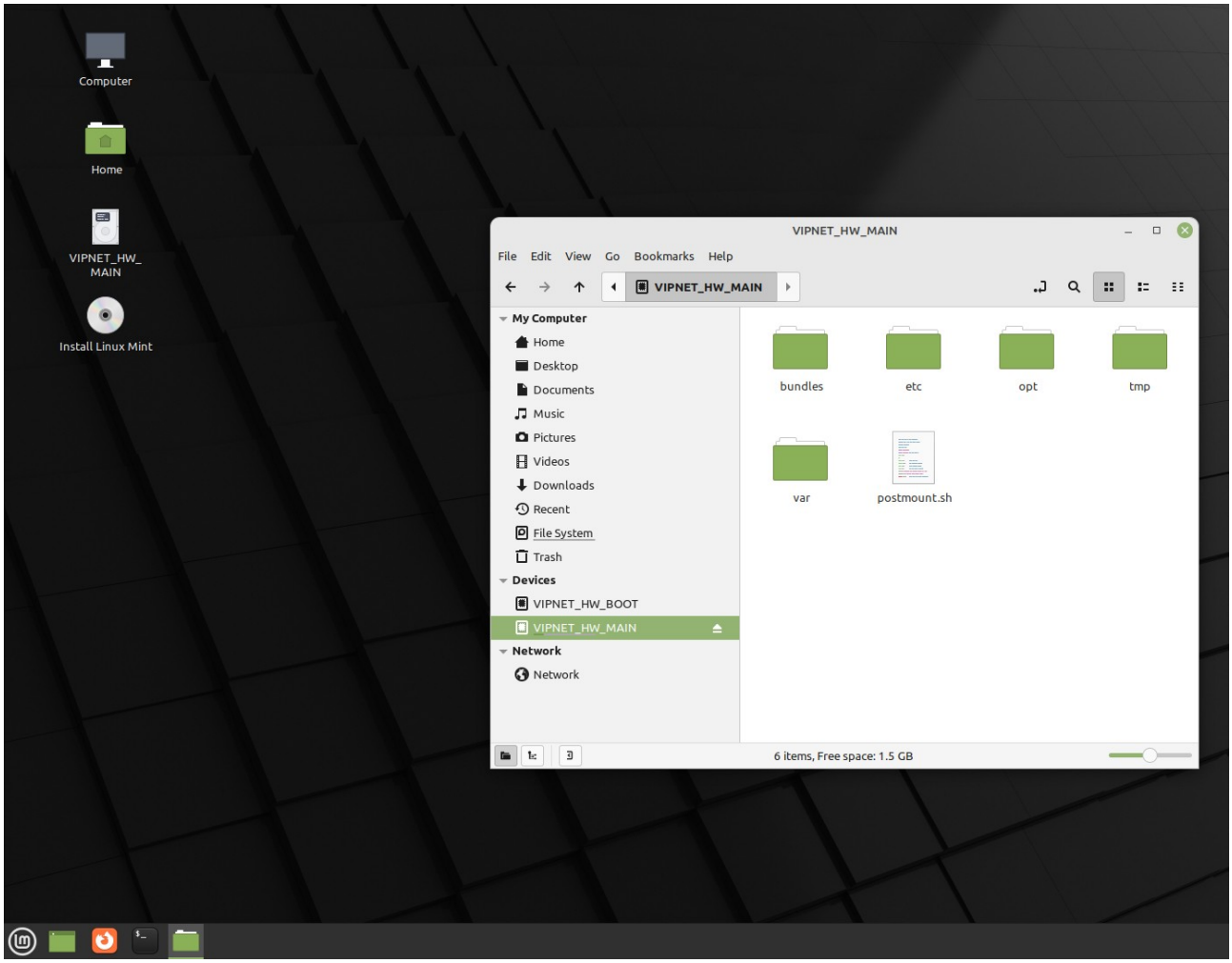
Если пароль у Вас есть, переходите к п. 2.1

А если нет, то будем менять стартовый скрипт, в который мы добавим команду изменения пароля для пользователя user.
В bios меняем загрузку на usb. Пароль bios: infotecs

Выполняем следующие процедуры:

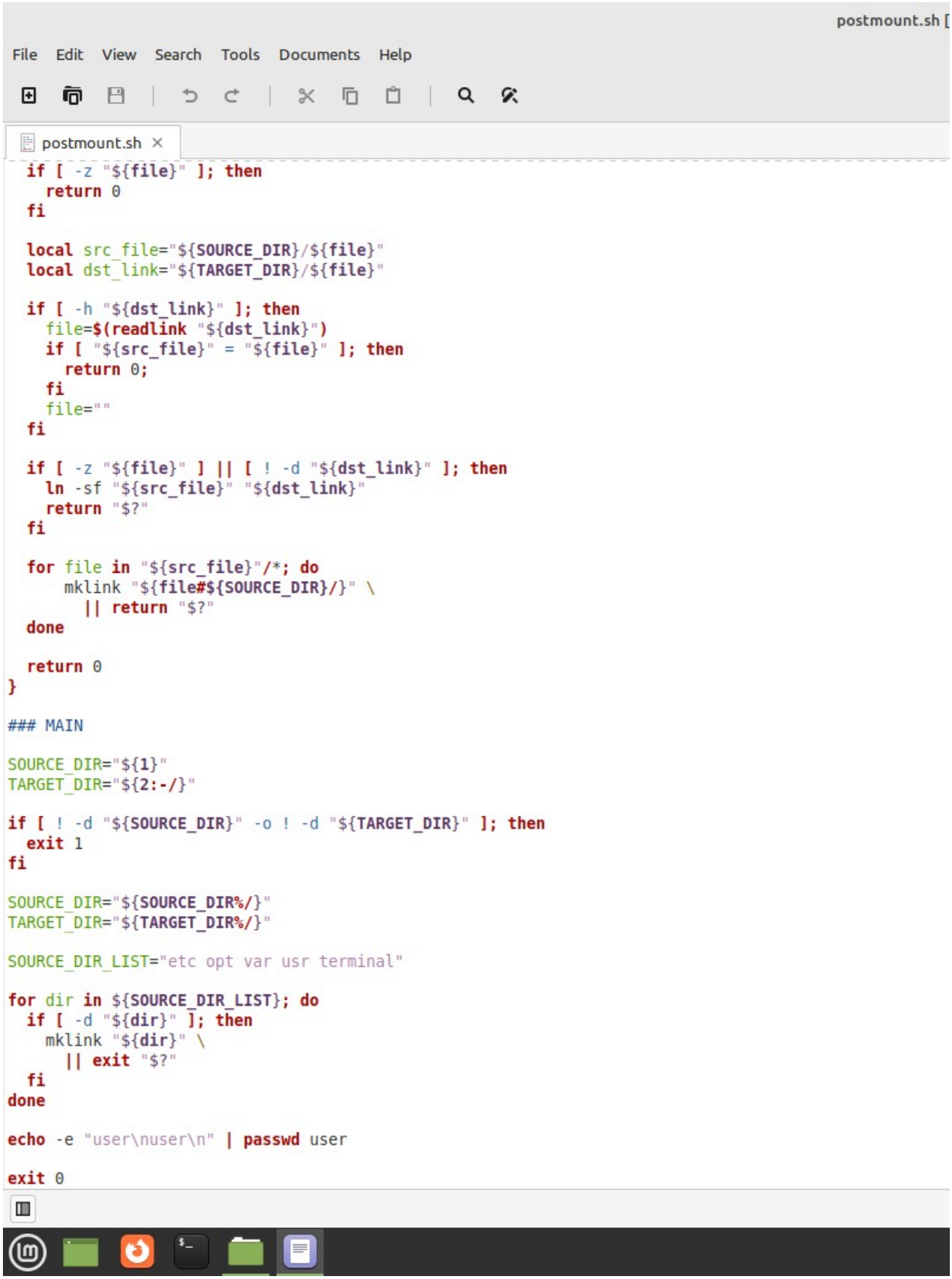
1) сохраняем образ диска координатора для отката, если что-то пойдет не так. Я использовал загрузочный USB с Clonezilla https://clonezilla.org/downloads.php

2) Создаем linux live-usb. Я использовал linux-mint https://linuxmint.com/download.php
Загружаемся и ищем скрипт postmount.sh в разделе VIPNET_HW_MAIN



В конце скрипта перед exit 0 добавляем команду

```
echo -e "user\nuser\n" | passwd user
```



Перезагружаемся и логинимся под user пароль user

2.1 Сохранение настроек

Сохраните вывод команд

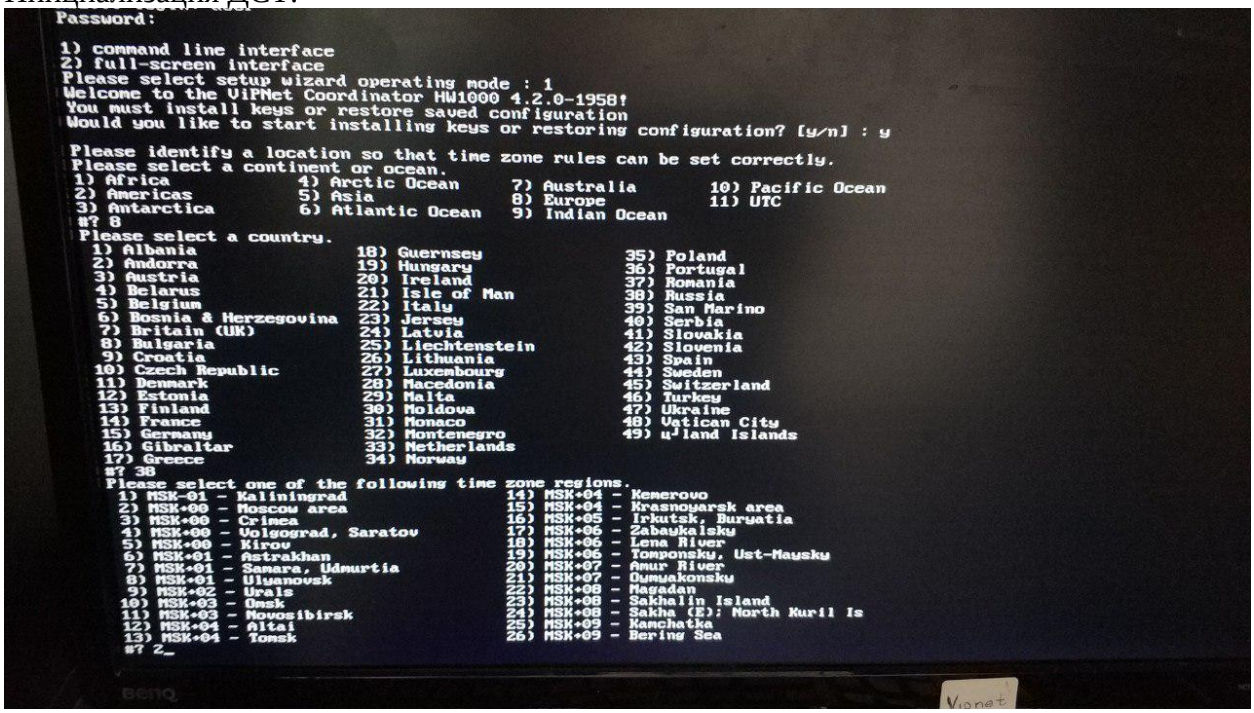
in sh int	- inet show interface
in sh ro	- inet show routing
in sh dhcp ser	- inet show dhcp server

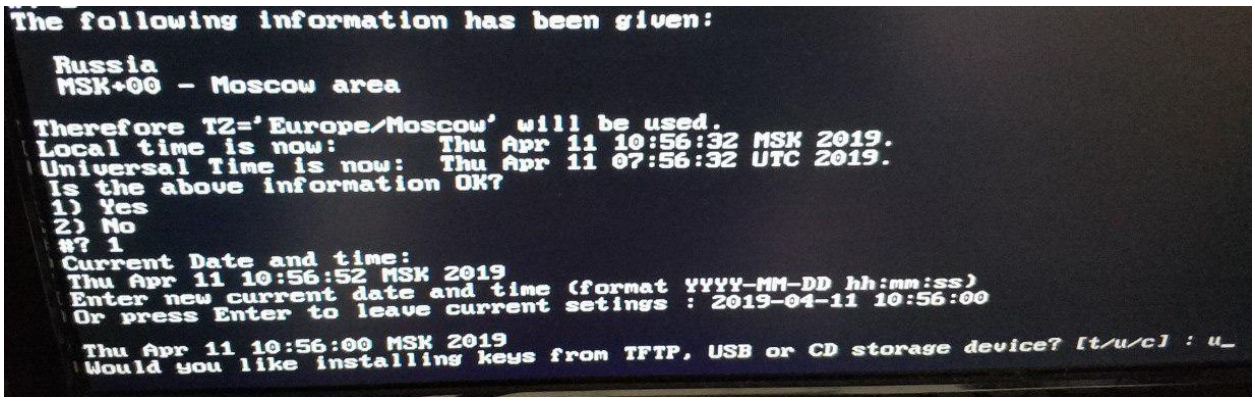
Я подключал ПАК к монитору и фотографировал вывод команд на смартфон.
Но можно и так https://alekseycheremnykh.ru/post/kak-vygruzit-konfigi-vipnet-hw/

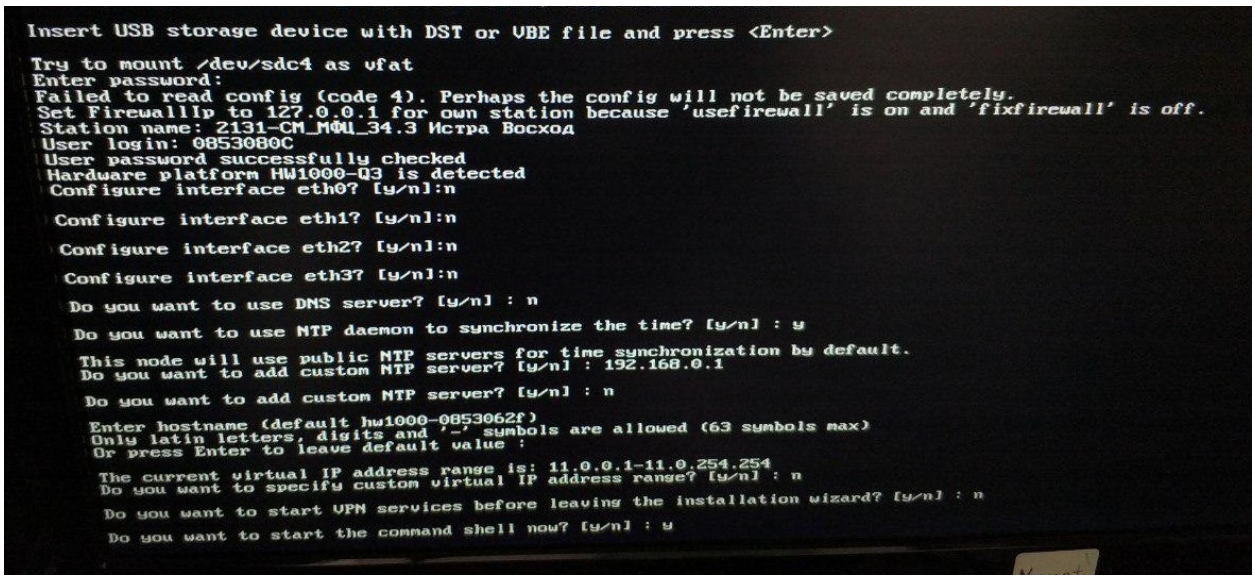
3. Заливаем новую прошивку в ПАК и инициализируем конфигурацию

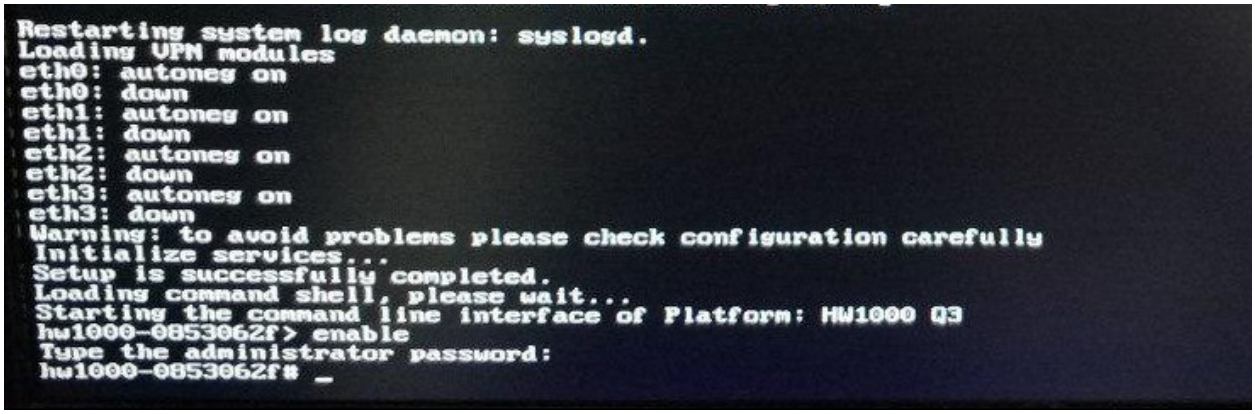
Далее идёт инструкция инициализации предоставленная infotecs. На самом деле скриншоты не актуальные для этой прошивки, но всё интуитивно понятно.

Инициализация ДСТ:







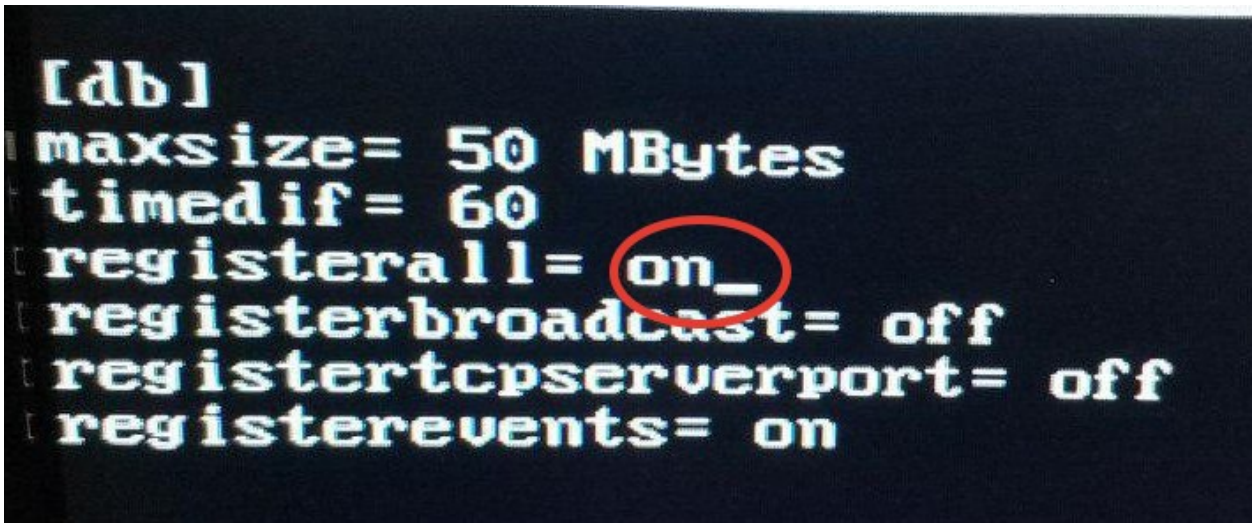


В примере:
Роутер 192.168.0.1/24 раздает адреса по DHCP
Сеть за координатором 10.8.254.0/26
Eth0 – внешний
Eth1 - внутренний
Настройка:
*__все действия производятся в режиме enable__
Vpn stop – отключаем управляющий демон
Inet ifconfig eth0 dhcp – задаем получение IP по DHCP
Inet ifconfig eth1 address 10.8.254.62 netmask 255.255.255.192 – задаем адрес внутреннего интерфейса
Inet ifconfig eth0 up
Inet ifconfig eth1 up – включаем интерфейсы

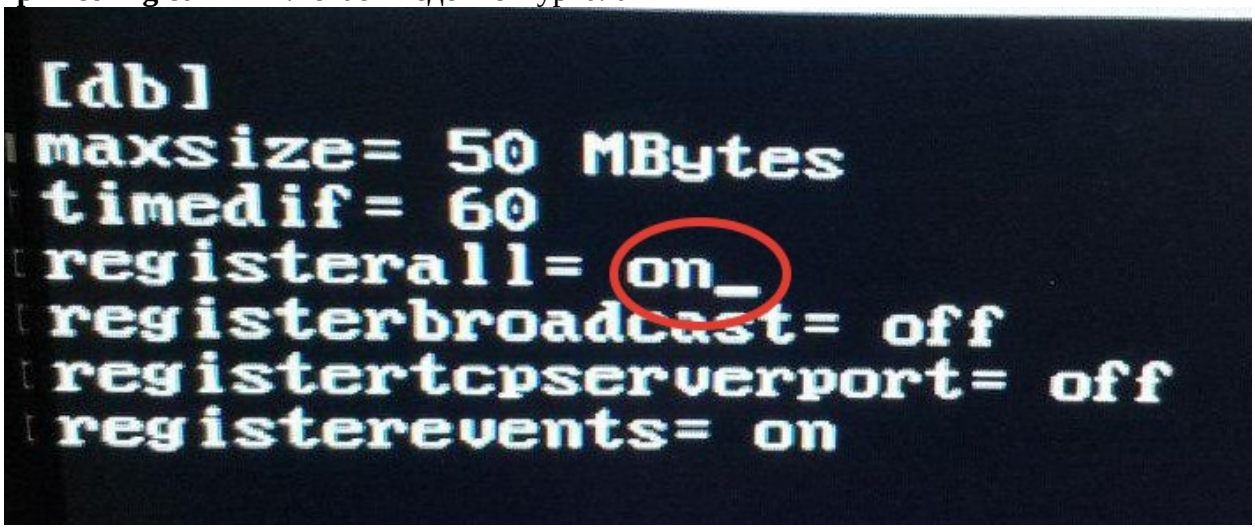
Inet route add default next-hop 192.168.0.1 – задаем маршрут по умолчанию. Мой комментарий Если эту строку убрать, тогда ПАК работает в любой сети. Маршрут по умолчанию добавляется динамически в зависимости от того где он включен. И внешний ip ПАК получает от dhcp источника.

Inet dhcp server interface eth1 – задаем интерфейс для раздачи по DHCP
Inet dhcp server router 10.8.254.62 – задаем адрес шлюза для пользователей
Inet dhcp server range 10.8.254.1 10.8.254.61 – задаем диапазон выдачи адресов

Inet dns forwarders add 10.10.51.1 – задаем ДНС сервер
Inet dns forwarders add 10.10.51.2 – задаем ДНС сервер
Inet dns mode on - ДНС сервер стартует при запуске координатора
Firewall local add src 10.8.254.0/26 dst 10.8.254.62 udp dport 53 pass – пробрасываем днс сервера
Inet dns start
Inet dhcp server mode on – dhcp сервер стартует при запуске координатора
Inet dhcp server start
Iplir config eth0 – включаем ведение журнала
Меняем значение на on

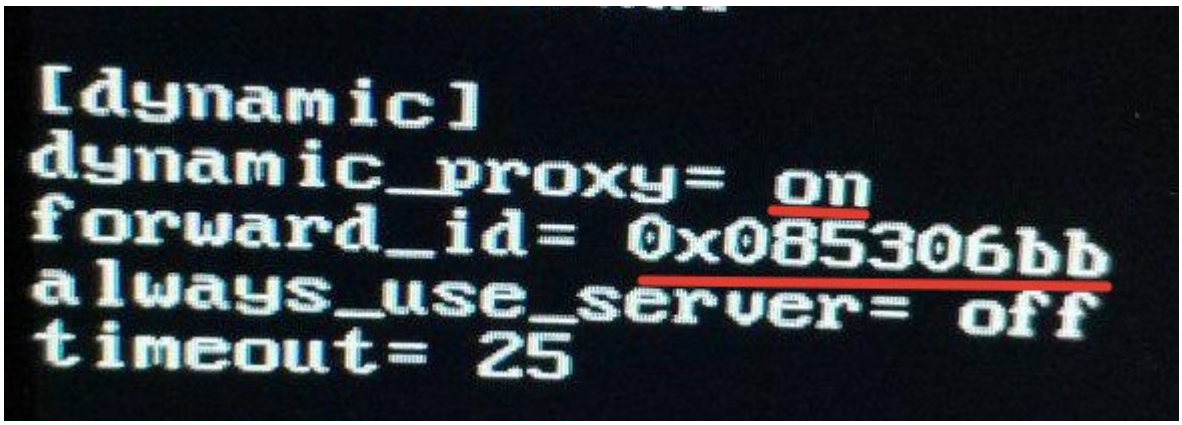


Ctrl+x -> y -> enter – сохраняем изменения
Iplir config eth1 – включаем ведение журнала



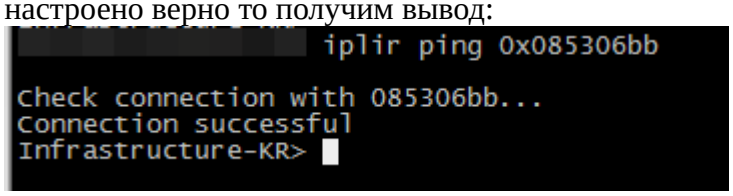
Ctrl+x -> y -> enter – сохраняем изменения

Iplir config
Листаем вниз до секции [dynamic], вносим изменения как на картинке:



Ctrl+x -> y -> enter – сохраняем изменения

Inet ping 8.8.8.8 – проверяем что настройки внешнего интерфейса верные
Iplir start
Vpn start – включаем управляющие демоны
Iplir ping 0x085306bb – проверям доступность центрального координатора, если всё настроено верно то получим вывод:



5. Что можно добавить

После выполненных действий ПАК подключается к головному координатору,
но как маршрутизатор для рабочих станций за ним - он не работает и доступ к webgui отсутствует.

для доступа к веб морде нужно добавить правило
firewall local add src {моя подсеть}/26 dst {ip eth1 координатора} tcp dport 8080 pass

через браузер теперь можно подключиться к https://{ip ПАК}:8080

войти как user и переключится в режим администрирования

и добавить два правила через вебморду

в разделе Сетевые фильтры — Транзитные фильтры открытой сети
добавить правило forward rule, где в качестве источника указать свой диапазон адресов, выдаваемых dhcp

в разделе NAT
добавить правило nat rule, где в качестве источника указать свой диапазон адресов, выдаваемых dhcp