

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-utverzhdennii-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

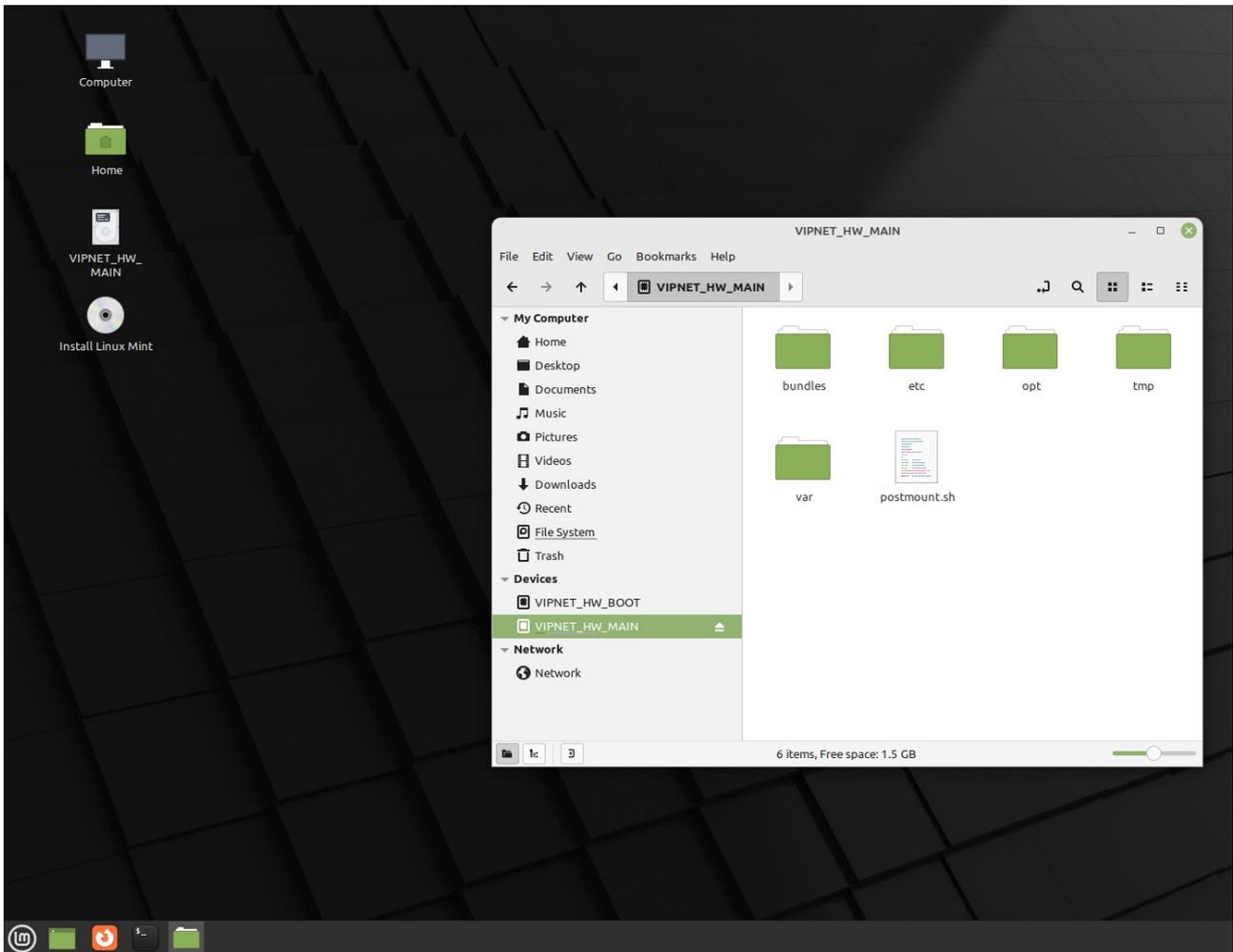
А если нет, то будем менять стартовый скрипт, в который мы добавим команду изменения пароля для пользователя user.

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

Сохраните вывод команд

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

Я подключаю ПАК к монитору и фотографирую 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:

```

Password:
1) command line interface
2) full-screen interface
Please select setup wizard operating mode : 1
Welcome to the ViPNet Coordinator HW1000 4.2.0-1958!
You must install keys or restore saved configuration
Would you like to start installing keys or restoring configuration? [y/n] : y

Please identify a location so that time zone rules can be set correctly.
Please select a continent or ocean.
1) Africa          4) Arctic Ocean      7) Australia      10) Pacific Ocean
2) Americas        5) Asia              8) Europe          11) UTC
3) Antarctica      6) Atlantic Ocean   9) Indian Ocean
#? 8

Please select a country.
1) Albania         18) Guernsey         35) Poland
2) Andorra         19) Hungary          36) Portugal
3) Austria         20) Ireland          37) Romania
4) Belarus         21) Isle of Man      38) Russia
5) Belgium         22) Italy             39) San Marino
6) Bosnia & Herzegovina 23) Jersey           40) Serbia
7) Britain (UK)   24) Latvia           41) Slovakia
8) Bulgaria        25) Liechtenstein    42) Slovenia
9) Croatia         26) Lithuania        43) Spain
10) Czech Republic 27) Luxembourg       44) Sweden
11) Denmark        28) Macedonia        45) Switzerland
12) Estonia        29) Malta             46) Turkey
13) Finland        30) Moldova           47) Ukraine
14) France          31) Monaco            48) Vatican City
15) Germany         32) Montenegro        49) u'land Islands
16) Gibraltar      33) Netherlands
17) Greece          34) Norway
#? 38

Please select one of the following time zone regions.
1) MSK-01 - Kaliningrad      14) MSK-04 - Kemerovo
2) MSK-00 - Moscow area     15) MSK-04 - Krasnoyarsk area
3) MSK-00 - Crimea         16) MSK-05 - Irkutsk, Buryatia
4) MSK-00 - Volgograd, Saratov 17) MSK-06 - Zabaykalsky
5) MSK-00 - Kirov           18) MSK-06 - Lena River
6) MSK-01 - Astrakhan       19) MSK-06 - Tomponsky, Ust-Mausku
7) MSK-01 - Samara, Udmurtia 20) MSK-07 - Amur River
8) MSK-01 - Ulyanovsk      21) MSK-07 - Oymyakonsky
9) MSK-02 - Urals           22) MSK-08 - Nagadan
10) MSK-03 - Omsk           23) MSK-08 - Sakhalin Island
11) MSK-03 - Novosibirsk    24) MSK-08 - Sakha (E); North Kuril Is
12) MSK-04 - Altai          25) MSK-09 - Kamchatka
13) MSK-04 - Tomsk         26) MSK-09 - Bering Sea
#? 2_

```

```

The following information has been given:

Russia
MSK+00 - Moscow area

Therefore TZ='Europe/Moscow' will be used.
Local time is now: Thu Apr 11 10:56:32 MSK 2019.
Universal Time is now: Thu Apr 11 07:56:32 UTC 2019.
Is the above information OK?
1) Yes
2) No
#? 1

Current Date and time:
Thu Apr 11 10:56:52 MSK 2019
Enter new current date and time (format YYYY-MM-DD hh:mm:ss)
Or press Enter to leave current settings : 2019-04-11 10:56:00

Thu Apr 11 10:56:00 MSK 2019
Would you like installing keys from TFTP, USB or CD storage device? [t/u/c] : u_

```

```
Insert USB storage device with DST or UBE file and press <Enter>
Try to mount /dev/sdc4 as vfat
Enter password:
Failed to read config (code 4). Perhaps the config will not be saved completely.
Set Firewall to 127.0.0.1 for own station because 'usefirewall' is on and 'fixfirewall' is off.
Station name: Z131-CN_M41_34.3 Метра Вокзод
User login: 0853080C
User password successfully checked
Hardware platform HW1000-Q3 is detected
Configure interface eth0? [y/n]:n
Configure interface eth1? [y/n]:n
Configure interface eth2? [y/n]:n
Configure interface eth3? [y/n]:n
Do you want to use DNS server? [y/n] : n
Do you want to use NTP daemon to synchronize the time? [y/n] : y
This node will use public NTP servers for time synchronization by default.
Do you want to add custom NTP server? [y/n] : 192.168.0.1
Do you want to add custom NTP server? [y/n] : n
Enter hostname (default hw1000-0853062f)
Only latin letters, digits and '-' symbols are allowed (63 symbols max)
Or press Enter to leave default value :
The current virtual IP address range is: 11.0.0.1-11.0.254.254
Do you want to specify custom virtual IP address range? [y/n] : n
Do you want to start VPN services before leaving the installation wizard? [y/n] : n
Do you want to start the command shell now? [y/n] : y
```

```
Restarting system log daemon: syslogd.
Loading VPN modules
eth0: autoneg on
eth0: down
eth1: autoneg on
eth1: down
eth2: autoneg on
eth2: down
eth3: autoneg on
eth3: down
Warning: to avoid problems please check configuration carefully
Initialize services...
Setup is successfully completed.
Loading command shell, please wait...
Starting the command line interface of Platform: HW1000 Q3
hw1000-0853062f> enable
Type the administrator password:
hw1000-0853062f# _
```

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

```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= on_
registerbroadcast= off
registertcpserverport= off
registerevents= on
```

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

Iplir config eth1 – включаем ведение журнала

```
[db]
maxsize= 50 MBytes
timedif= 60
registerall= on_
registerbroadcast= off
registertcpserverport= off
registerevents= on
```

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

Iplir config

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

```
[dynamic]
dynamic_proxy= on
forward_id= 0x085306bb
always_use_server= off
timeout= 25
```

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 – проверяем доступность центрального координатора, если всё настроено верно то получим вывод:

```
iplir ping 0x085306bb
check connection with 085306bb...
Connection successful
Infrastructure-KR> █
```

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