**Настройка Wi-Fi контроллера Mikrotik CAPsMAN и точек доступа CAP**

Задача: настроить сеть Wi-Fi точек доступа Mikrotik (Controlled Access Points - CAP) под управлением Wi-Fi контроллера Mikrotik (Controlled Access Point system Manager -CAPsMAN). Точки доступа должны иметь по 2 SSID (в VLAN 116 – SSID S\_Guest, в VLAN 115 – SSID DLG), и управляться в менеджмент VLAN 117 по проводной сети.

!!! В случае любой непонятной ситуации смотрим логи. Меню **Log**.

*Полезная статья на Mikrotik-Wiki -* [*https://wiki.mikrotik.com/wiki/Manual:CAPsMAN\_with\_VLANs*](https://wiki.mikrotik.com/wiki/Manual:CAPsMAN_with_VLANs)

**1. Настройка маршрутизатора-контроллера CAPsMAN (на базе виртуальной машины Mikrotik)**

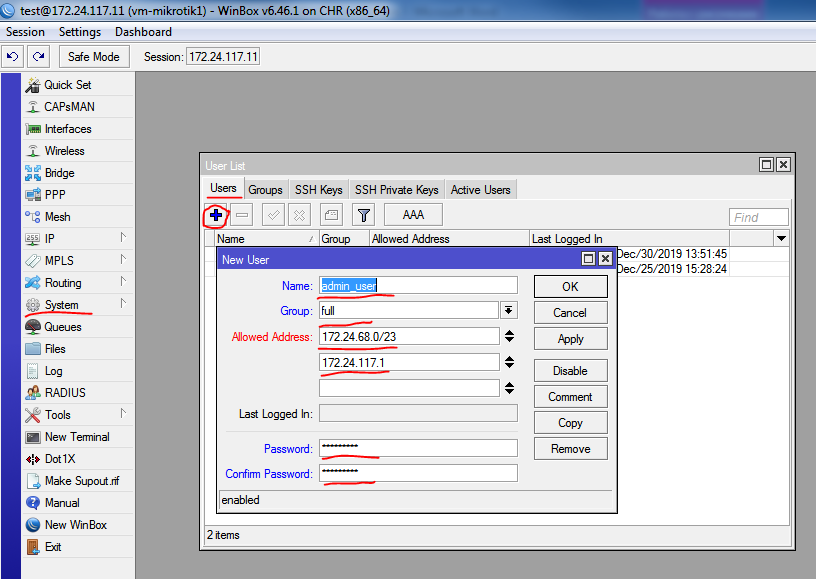
**1.1. Общие настройки.**

**1.1.1. Создаём пользователей для управления роутером.**

Создаем пользователей для управления роутером.

Доступ дадим только из подсети 172.24.68.0/23 и со шлюза сети управления – 172.24.117.1, - доступ на чтение и запись – full, придумываем пароль и подтверждаем.

В графическом интерфейсе:



*Рис. 1.1.1. Добавление системных пользователей*

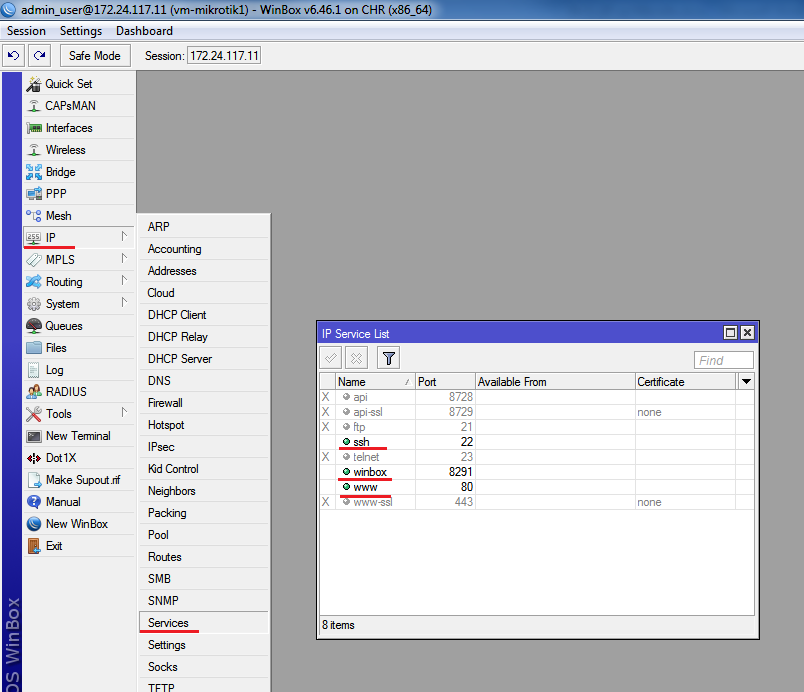
В консоли CLI:

user add name=*test* group=full password=*~~trololo~~*

После создания пользователей с полным доступом, заходим под ними и удаляем стандартного пользователя **admin**.

**1.1.2. Ограничиваем доступ к маршрутизаторы по ненужным портам – стандартным сервисам.**

В целях безопасности отключаем все ненужные TCP-сервисы, которые открыты снаружи по умолчанию:

*****Рис. 1.1.2. Отключение ненужных сервисов*

В консоли CLI:

ip service print

Flags: X - disabled, I - invalid

# NAME PORT ADDRESS CERTIFICATE

0 telnet 23

1 ftp 21

2 www 80

3 ssh 22

4 www-ssl 443 none

5 api 8728

6 winbox 8291

7 api-ssl 8729 none

ip service disable 0

ip service disable 1

ip service disable 4

ip service disable 5

ip service disable 7

ip service print

Flags: X - disabled, I - invalid

# NAME PORT ADDRESS CERTIFICATE

0 XI telnet 23

1 XI ftp 21

2 www 80

3 ssh 22

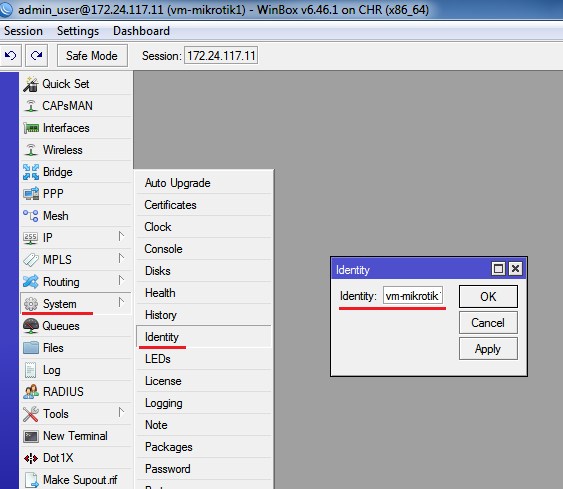
4 XI www-ssl 443 none

5 XI api 8728

6 winbox 8291

7 XI api-ssl 8729 none

**1.1.3. Настраиваем имя маршрутизатора.**



*Рис. 1.1.3. Имя маршрутизатора*

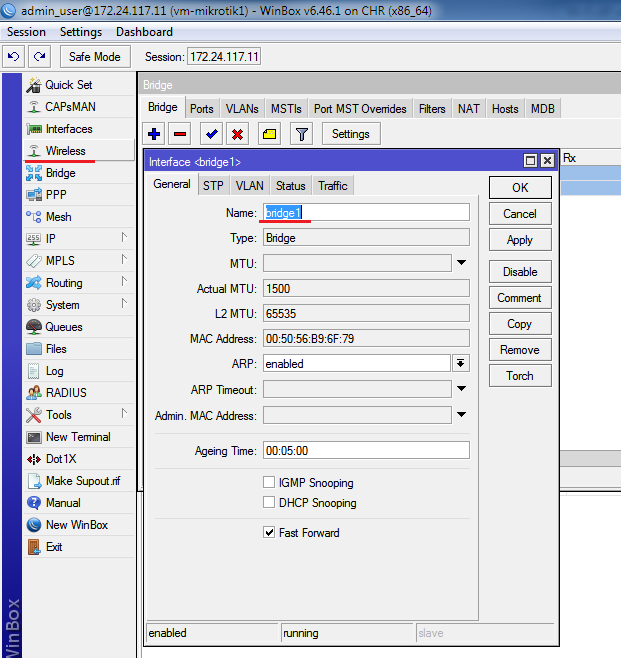
В консоли CLI:

system identity set name=vm-mikrotik1

**1.1.4. Создаём бридж для работы в режиме trunk и VLAN-интерфейсы с тегами VLAN-ов**

В терминологии Mikrotik, bridge – это программная реализация VLAN. Поэтому bridge позволяет объединять несколько физических интерфейсов в одну логическую группу.

Создаём новый виртуальный интерфейс – bridge1:

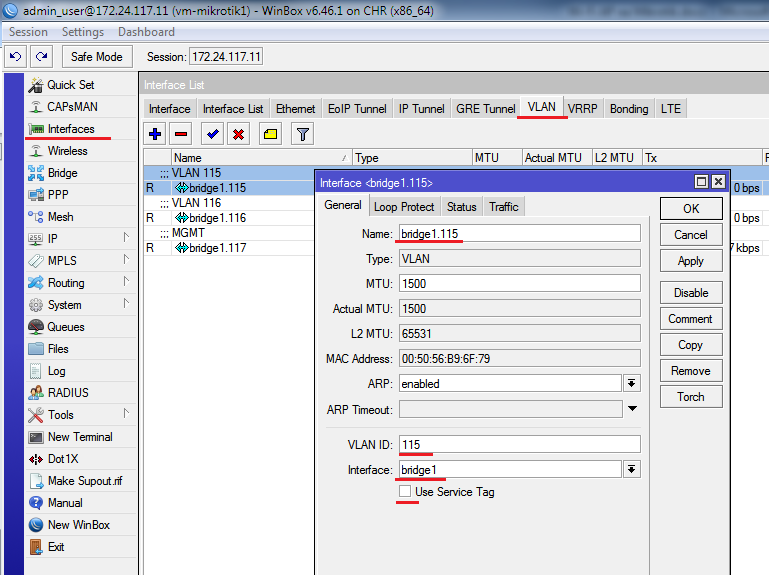
****

*Рис. 1.1.4. Добавление нового виртуального интерфейса bridge*

В консоли CLI:

interface bridge add comment="Trunk VLAN 115-117" name=bridge1

Создаём VLAN-интерфейсы с тегами нужных VLAN-ов. Делаем это для VLAN 115-117:



*Рис. 1.1.5. Добавление новых VLAN*

В консоли CLI:

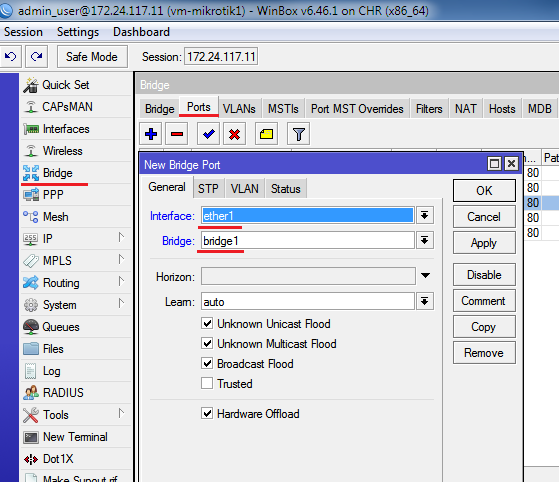
interface vlan add comment="VLAN 115" interface=bridge1 name=bridge1.115 vlan-id=115

interface vlan add comment="VLAN 116" interface=bridge1 name=bridge1.116 vlan-id=116

interface vlan add comment=MGMT interface=bridge1 name=bridge1.117 vlan-id=117

**1.1.5. Вешаем бридж интерфейс на Ethernet интерфейс**

На нашем виртуальном Mikrotik нам будет достаточно использовать один Ethernet интерфейс, на который будет назначен виртуальный интерфейс bridge (виртуальная группа интерфейсов), к которому в свою очередь привязаны тегированные VLAN-ы.

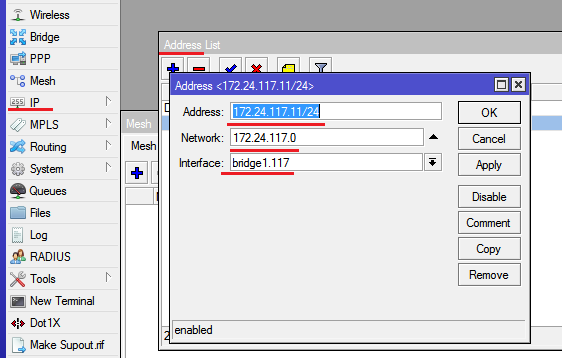
****

*Рис. 1.1.6. Добавление порта Ether1 в виртуальную группу bridge1*

В консоли CLI:

interface bridge port add bridge=bridge1 interface=ether1

**1.1.6. Настраиваем IP-адрес управления роутером**

****

*Рис. 1.1.7. Настройка management IP-адреса на интерфейсе с VLAN 117*

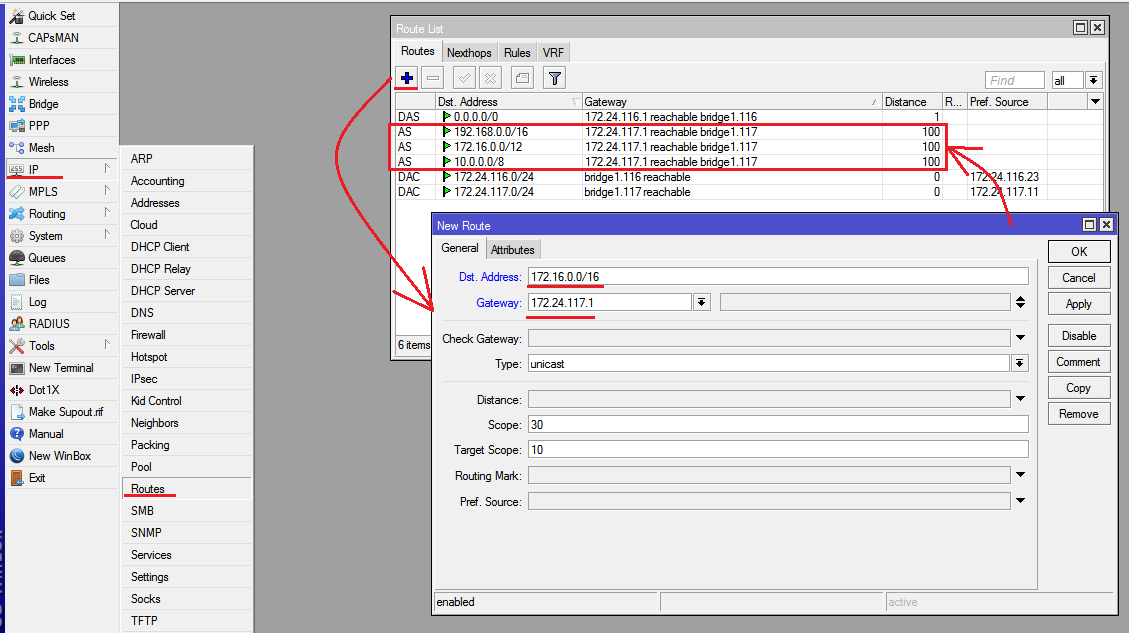
В консоли CLI:

ip address add address=172.24.117.11/24 interface=bridge1.117 network=172.24.117.0

**1.1.7. Добавляем обратный маршрут в сеть Банка**

Нужны маршруты к сетям:

172.16.0.0/12, 192.168.0.0/16, 10.0.0.0/8.

****

*Рис. 1.1.8. Настройка статических маршрутов во внутреннюю сеть Банка*

В консоли CLI:

ip route add distance=100 dst-address=10.0.0.0/8 gateway=172.24.117.1

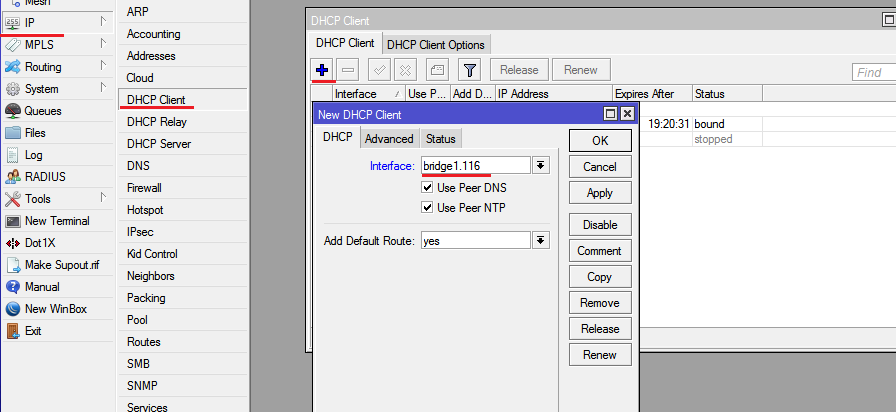
ip route add distance=100 dst-address=172.16.0.0/12 gateway=172.24.117.1

ip route add distance=100 dst-address=192.168.0.0/16 gateway=172.24.117.1

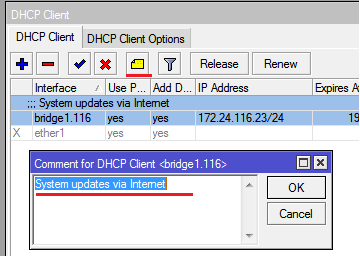
**1.1.8. Обновляем прошивку маршрутизатора до последней стабильной**

Выход в Интернет из сети управления - VLAN 117, - заблокированы zone-based firewall.

Поэтому для обновления прошивки временно создадим DHCP клиента на любом из других VLAN, предназначенных для доступа в Интернет по Wi-Fi: VLAN 115, 116.



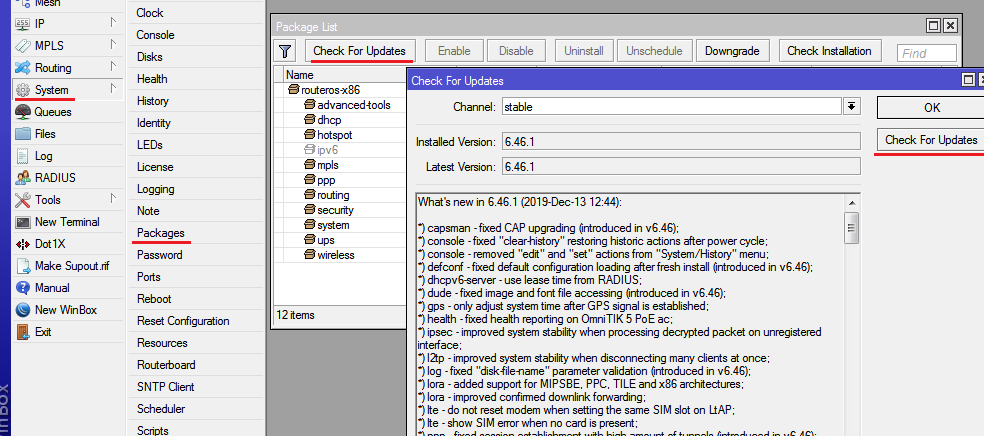
*Рис. 1.1.9. Настройка DHCP клиента для обновлений софта*



*Рис. 1.1.10. Добавление комментария к клиенту DHCP*

В консоли CLI:

ip dhcp-client add comment="System updates via Internet" disabled=no interface=bridge1.116



*Рис. 1.1.11. Проверка обновлений софта системы*

В консоли CLI:

system package update check-for-updates

channel: stable

installed-version: 6.46.1

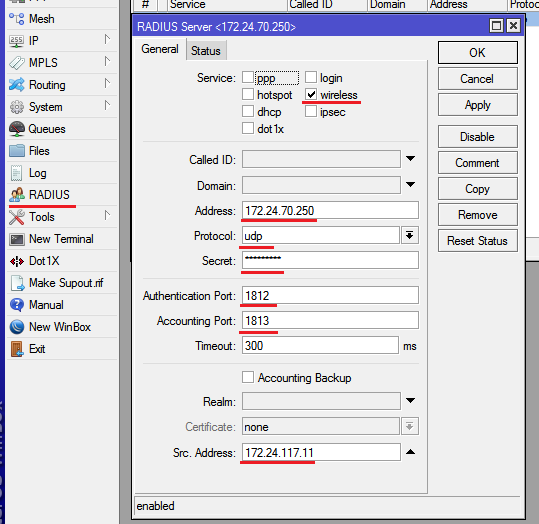
latest-version: 6.46.1

status: System is already up to date

В нашем случае система обновлена до последней стабильной версии, поэтому обновление не требуется. Но в целом система обновляется очень легко. Если бы нашлась более свежая версия ПО, то, нажав кнопку “Download & Update”, мы обновились бы до новой прошивки. Маршрутизатор при этом перезагружается!!!

**1.2. Настраиваем RADIUS клиент для аутентификации пользователей на точках доступа**

Клиент RADIUS будет использоваться для аутентификации пользователей, подключающихся к точкам доступа CAP.



*Рис. 1.2.1. Настройка клиента RADIUS*

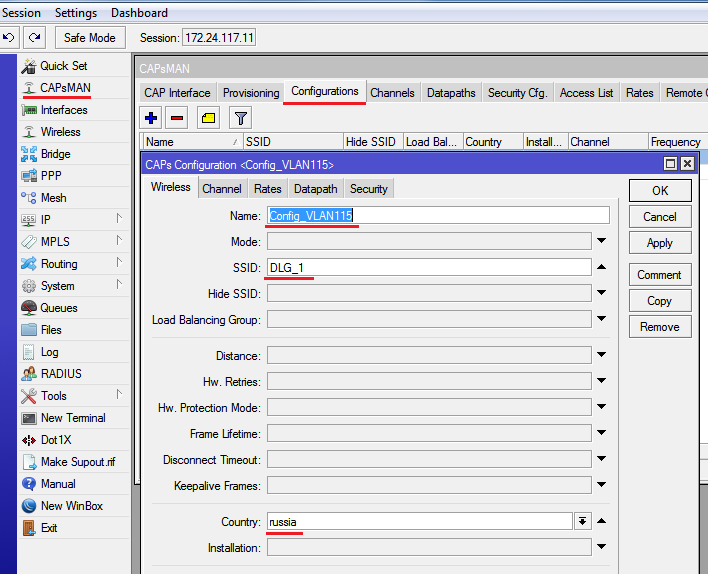
В консоли CLI:

radius add address=172.24.70.250 secret=*~~some-secret~~* service=wireless src-address=172.24.117.11

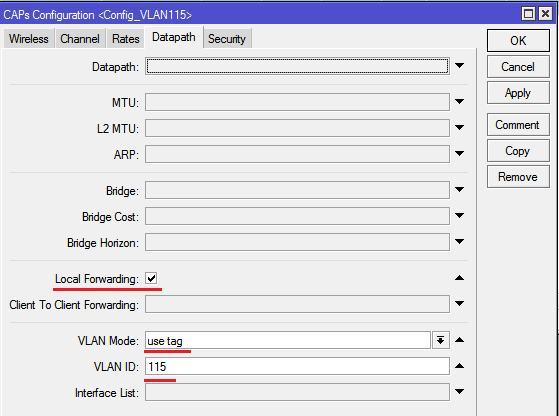
**1.3. Настраиваем непосредственно CAPsMAN**

**1.3.1. Настраиваем конфигурационные профили для двух SSID**

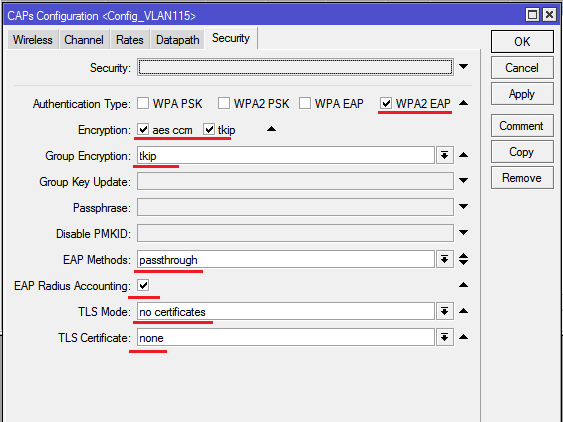
Настраиваем сначала конфигурацию для обоих SSID. В нашем случае при подключении к SSID DLG\_1 должно выполняться правило – прокинуть пользователя в VLAN 115, а при подключении к S\_Guest1 – в VLAN 116. Чтобы трафик пользователей коммутировался уже на точках доступа, ставим режим Local Forwarding. Это добавляет метку VLAN (в нашем случае 115 и 116) уже при попадании на точку доступа. Иначе трафик от CAP шел бы к CAPsMAN со специальной проприетарной меткой Mikrotik, а уже на контроллере – роутере в режиме CAPsMAN – ставилась бы метка VLAN. В нашей сети используется RADIUS сервер для аутентификации и авторизации, поэтому режим аутентификации выбираем EAP, а метод – paththrough – так как сервер находится не на самом роутере Mikrotik CAPsMAN.



*Рис. 1.3.1. Конфигурация профиля Config\_VLAN115 для SSID DLG\_1 - WiFi*



*Рис. 1.3.2. Конфигурация профиля Config\_VLAN115 для SSID DLG\_1 – передача данных*



*Рис. 1.3.3. Конфигурация профиля Config\_VLAN115 для SSID DLG\_1 – безопасность подключения*

Аналогичные настройки будут и для профиля Config\_VLAN116, за исключением имени SSID и VLAN тега.

В консоли CLI:

caps-man configuration add country=russia datapath.local-forwarding=yes datapath.vlan-id=115 datapath.vlan-mode=use-tag name=Config\_VLAN115 security.authentication-types=wpa2-eap security.eap-methods=passthrough security.eap-radius-accounting=yes \

security.encryption=aes-ccm,tkip security.group-encryption=tkip security.tls-certificate=none security.tls-mode=no-certificates ssid=DLG\_1

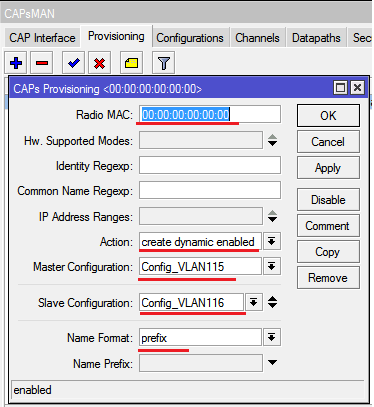
caps-man configuration add country=russia datapath.local-forwarding=yes datapath.vlan-id=116 datapath.vlan-mode=use-tag name=Config\_VLAN116 security.authentication-types=wpa2-eap security.eap-methods=passthrough security.eap-radius-accounting=yes \

security.encryption=aes-ccm,tkip security.group-encryption=tkip security.tls-certificate=none security.tls-mode=no-certificates ssid=S\_Guest1

**1.3.2. Настраиваем правила распространения для точек доступа**

В правилах распространения мы укажем – для всех MAC адресов, то есть без ограничений (default).

Master Configuration профиль будет применена к физическим интерфейсам удаленных CAP, а все Slave Configuration профили будут настраиваться на виртуальных интерфейсах, которые будут создаваться по мере надобности автоматически.



*Рис. 1.3.4. Настройка распространения*

В консоли CLI:

caps-man provisioning add action=create-dynamic-enabled master-configuration=Config\_VLAN115 name-format=prefix slave-configurations=Config\_VLAN116

На этом наша настройка CAPsMAN закончена.

**2. Настройка точек доступа CAP (на базе маршрутизаторов Mikrotik RB952Ui-5ac2nD)**

Общие настройки для точек доступа практически не отличаются от настроек контроллера.

Только есть несколько нюансов:

1. В группу bridge1 добавляем интерфейсы Ether1, Ether5 (UpLink), wlan1 и wlan2.

2. Интерфейс Ether1 по умолчанию состоит в списке WAN (**Interfaces ---> Interface List**). Нужно удалить его из этого списка, так как в настройках файерволла есть правила для списка WAN.

В данной инструкции в качестве физического UpLink используется Ether5, но на практике будет использован Ether1, так как у него есть функция PoE-in.

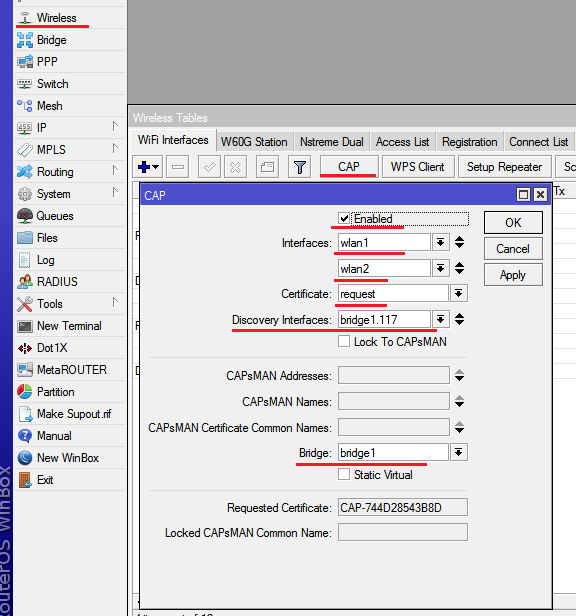
3. Интерфейс VLAN – bridge1.117 – добавляем в список интерфейсов LAN, чтобы стандартные правила файерволла применились к нему.

В консоли CLI:

interface list member add interface=bridge1.117 list=LAN

4. Имена систем будут AP.12, AP.13.

Сразу перейдем к настройке самих CAP.



*Рис. 2.1. Настройка CAP*

В консоли CLI:

interface wireless cap set bridge=bridge1 certificate=request discovery-interfaces=bridge1.117 enabled=yes interfaces=wlan1,wlan2

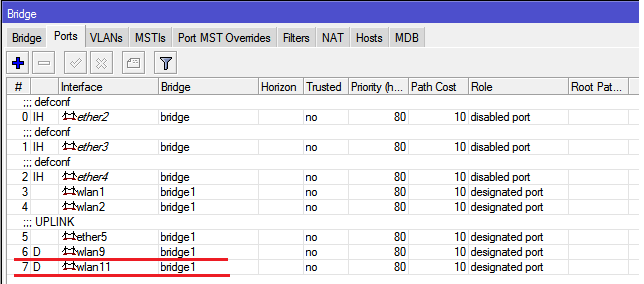
На этом настройка CAP закончена!

**3. Как с ними работать. Анализ, диагностика, общие принципы, нюансы.**

!!! В случае любой непонятной ситуации смотрим логи. Меню **Log**.

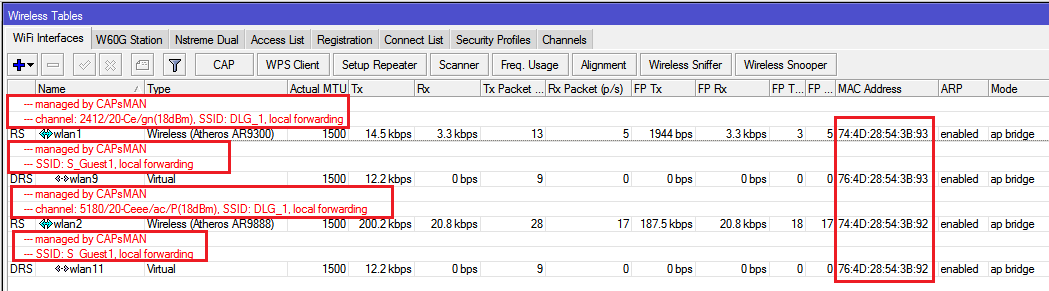
**3.1. Точка доступа CAP. Анализ, диагностика, общие принципы, нюансы.**

Так как мы привязали настройку CAP к bridge1, то виртуальные интерфейсы, создаваемые менеджером (CAPsMAN) будут соответствовать bridge1:



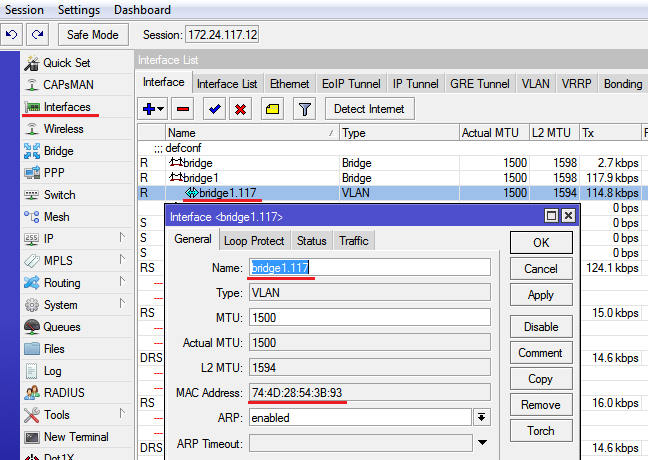
*Рис. 3.1.1. Виртуальные Wi-Fi интерфейсы – члены группы bridge1*

Wi-Fi интерфейсы создаются с комментариями. MAC адреса интерфейсов тоже можно посмотреть тут (**Wireless --> WiFi Interfaces**):

 *Рис. 3.1.2. Виртуальные Wi-Fi интерфейсы – члены группы bridge1*

В целом, на точке доступа CAP по диагностике и нюансам все ищется в разделе **Wireless --> WiFi Interfaces**.

На CAPsMAN точка доступа CAP будет видна с МАС-адресом интерфейса, который включен как *Discovery Interface* в настройках **Wireless ---> CAP**, то есть bridge1.117:



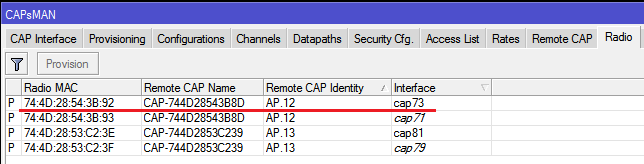
*Рис. 3.1.3. Просмотр МАС-адреса интерфейса обнаружения на CAP*

**3.2. Менеджер CAPsMAN. Анализ, диагностика, общие принципы, нюансы.**

Теперь мы заходим в панель управления маршрутизатором, настроенного в качестве CAPsMAN.

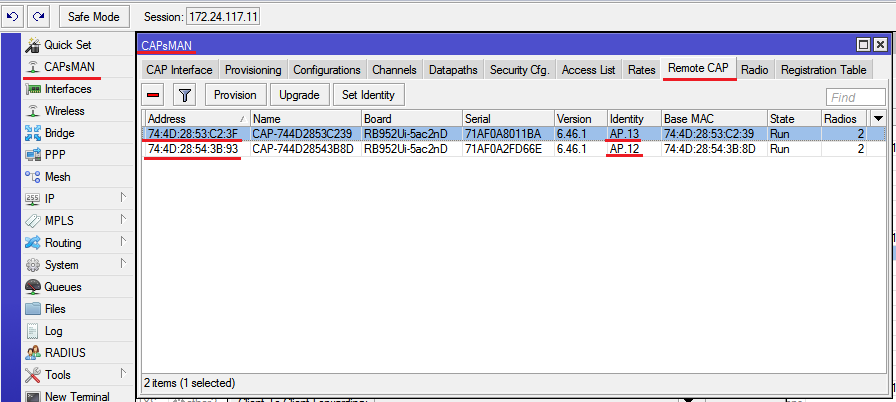
В нашем случае – это виртуальная машина. Напомню, что наши точки настроены в режиме *Local Forwarding* (смотри рисунок 1.3.2.), то есть с маршрутизатора на UpLink уходит трафик с тегом VLAN и без специального проприетарного тега CAPsMAN.

Чтобы увидеть соответствие CAP-интерфейсов реальным удаленным точкам доступа, нужно зайти в меню **CAPsMAN ---> Radio.** Здесь видно и имя удаленной точки доступа, и MAC-адрес соответствующего её Wi-Fi интерфейса, и её уникальное CAP имя, и, собственно, название интерфейса на роутере CAPsMAN:

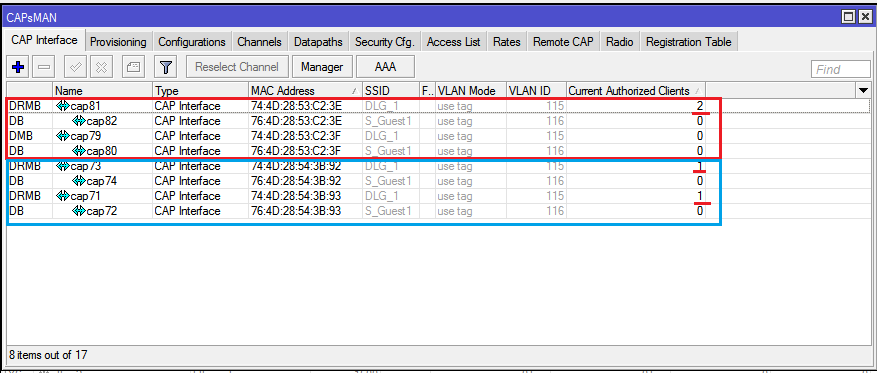


*Рис. 3.2.2. Радиоинтерфейсы CAPsMAN и их физические интерфейсы (CAPsMAN ---> Radio)*

Посмотреть, какие CAP подключены в данный момент к CAPsMAN, можно в меню **CAPsMAN ---> Remote CAP**. Тут можно увидеть из особо полезного – имя удаленной точки (Identity) и адрес, который, в случае с подключением в одной широковещательном домене, будет соответствовать MAC адресу интерфейса обнаружения удаленной точки (смотри рисунок 3.1.2):

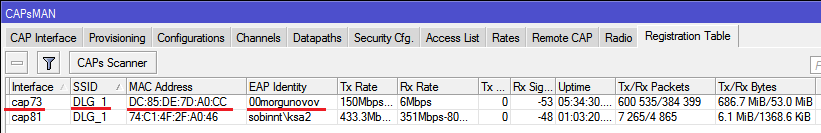
*****Рис. 3.2.2. Подключенные точки доступа (CAPsMAN ---> Remote CAP)*

В меню **CAPsMAN ---> CAP Interface** можно проверить все созданные CAP интерфейсы, проверить по МАС-адресу, какой физической точке и какому интерфейсу удаленной точки соответствует определенный интерфейс CAP, а также число подключенных авторизованных пользователей.



*Рис. 3.2.3. CAP интерфейсы CAPsMAN (CAPsMAN ---> CAP Interface)*

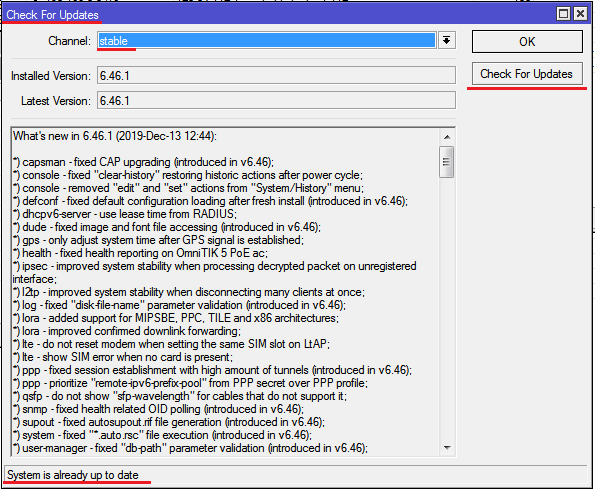
Всех подключенных пользователей можно посмотреть в разделе **CAPsMAN ---> Registration Table**:

 *Рис. 3.2.4. Подключенные пользователи (CAPsMAN ---> Registration Table)*

**3.2.1. Менеджер CAPsMAN. Прошивка самого роутера CAPsMAN и удалённых точек доступа.**

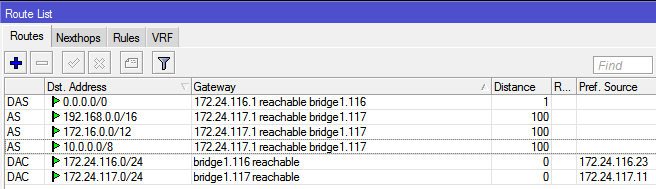
!!! В случае любой непонятной ситуации смотрим логи. Меню **Log**.

Для того, чтобы обновить прошивку самого роутера, нужно зайти в меню **System ---> Packages ---> Check For Updates** и нажать кнопку*Check For Updates*.



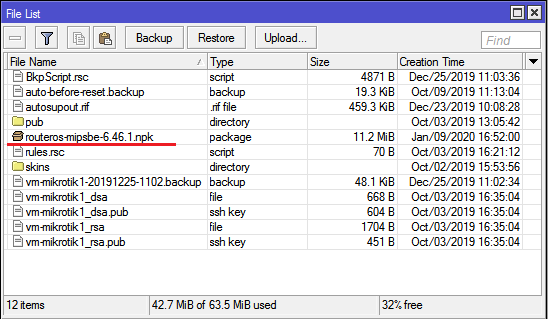
*Рис. 3.2.5. Обновление прошивки маршрутизатора локально*

Нюанс! Так как на подсеть управления роутером (VLAN 117) у нас установлены ограничения на межсетевом экране, был поднят DHCP-клиент на интерфейсе с VLAN 116. Шлюз по умолчанию прилетает автоматически и с другими настройками, а внутренние сети статически прописаны через шлюз VLAN117.



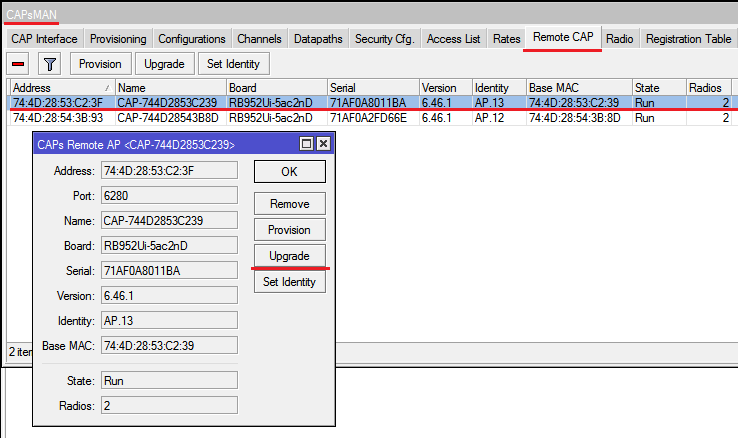
*Рис. 3.2.6. Маршруты на роутере CAPsMAN*

Чтобы обновить удалённую точку доступа, необходимо скачать прошивку, например, на ПК и загрузить её в файловое хранилище роутера-мастера CAPsMAN. Делается это в меню **Files ---> Upload…** После загрузки файл прошивки будет виден в файлах роутера:



*Рис. 3.2.7. Файл прошивки в файловом хранилище роутера CAPsMAN*

Теперь заходим **CAPsMAN ---> Remote CAP** и дважды щелкаем по необходимой удаленной точке доступа. Затем жмём кнопку Upgrade:



*Рис. 3.2.8. Обновление прошивки удаленной точки доступа*

Процесс обновления удаленной точки доступа можно посмотреть в логах роутера CAPsMAN (меню **Log**):



*Рис. 3.2.9. Логи обновления удалённой точки доступа CAP*